Personuppgiftsbiträdesavtal

mellan Södermalms stadsdelsnämnd, nedan kallad Personuppgiftsansvarig och Klicka eller tryck här för att ange text. **(leverantör), nedan kallad Personuppgiftsbiträde.**

Detta Personuppgiftsbiträdesavtal, jämte Instruktioner och en eventuell förteckning över Underbiträden, är en bilaga till parternas Huvudavtal 2024-xx-xx angående Drift av Södermalms grupp- och servicebostäder samt Teckentullens dagliga verksamhet med diarienummer SÖD 2022/1467.

1. Bakgrund

Enligt Europaparlamentets och rådets förordning (EU) 2016/679 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 (”Dataskyddsförordningen”) ska det finnas ett skriftligt avtal mellan Personuppgiftsansvarig och Personuppgiftsbiträde avseende den behandling av personuppgifter som Personuppgiftsbiträdet ska utföra för Personuppgiftsansvarigs räkning.

Detta Personuppgiftsbiträdesavtal mellan Personuppgiftsansvarig och Personuppgiftsbiträde (nedan ”Parterna”) reglerar hur Personuppgiftsbiträdet får behandla personuppgifter för Personuppgiftsansvarigs räkning. Personuppgiftsbiträdesavtalet utgör en bilaga till Huvudavtalet, men utgör samtidigt ett självständigt avtal. I händelse av motstridig lydelse mellan bestämmelserna om personuppgiftsbehandling i Personuppgiftsbiträdesavtalet och Huvudavtalet har Personuppgiftsbiträdesavtalet företräde. I fall av gällande standardavtalsklausuler för tredjelandsöverföring har dock standardavtalsklausulerna företräde i händelse av motstridig lydelse med detta Personuppgiftsbiträdesavtal eller Huvudavtalet.

2. Definitioner

Begreppen ”Personuppgiftsansvarig”, ”Personuppgiftsbiträde”,” samt andra begrepp i detta Personuppgiftsbiträdesavtal, som är relaterade till behandling av personuppgifter, ska tolkas och tillämpas i enlighet med vad som följer av Dataskyddsförordningen.

Med ”Standardavtalsklausuler” avses EU-kommissionens beslutade standardavtalsklausuler.

3. Behandling av personuppgifter

Allmänt om personuppgiftsbehandlingen

Personuppgiftsbiträdet och personer som agerar för Personuppgiftsbiträdets räkning får endast behandla personuppgifter i enlighet med Personuppgiftsbiträdesavtalet inklusive de skriftliga instruktioner som Personuppgiftsansvarig lämnar, samt ”Tillämplig lag” varmed avses gällande nationell och EU-lagstiftning avseende dataskydd som gäller för personuppgiftsbehandlingen inom ramen för Personuppgiftsbiträdesavtalet.

Om Personuppgiftsbiträdet finner att instruktioner är otydliga, i strid med Tillämplig lag eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera Personuppgiftsansvarig om detta och därefter invänta vidare instruktioner från Personuppgiftsansvarig.

Utöver de skyldigheter som Personuppgiftsbiträdet har enligt Tillämplig lag ska Personuppgiftsbiträdet även följa den uppförandekod eller certifiering som Personuppgiftsbiträdet har åtagit sig att följa.

Säkerhet vid personuppgiftsbehandling

Personuppgiftsbiträdet ska vidta alla åtgärder som krävs enligt artikel 32 Dataskyddsförordningen. Det innebär att Personuppgiftsbiträdet ska implementera och löpande säkerställa lämpliga tekniska och organisatoriska åtgärder i enlighet med detta Personuppgiftsbiträdesavtal inklusive instruktioner och Tillämplig lag i syfte att skydda personuppgifter från 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. Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera de

tekniska och organisatoriska åtgärder som ska säkerställa personuppgiftsbehandlingens säkerhet. Notera att lämpliga åtgärder även inkluderar Personuppgiftsbiträdets förmåga att upptäcka och hantera eventuell personuppgiftsincident.

Personuppgiftsbiträdet ska bistå Personuppgiftsansvarig genom lämpliga tekniska och organisatoriska åtgärder, så att Personuppgiftsansvarig kan fullgöra sin skyldighet enligt Tillämplig lag.

Personuppgiftsbiträdet ska bistå Personuppgiftsansvarig med att tillse att skyldigheterna enligt artiklarna 32-36 i Dataskyddsförordningen fullgörs, inklusive vara behjälplig med genomförandet av konsekvensbedömning avseende dataskydd.

Tredjelandsöverföring i samband med personuppgiftsbehandling

Personuppgiftsbiträdet ska säkerställa att personuppgifterna behandlas inom EU/EES. Personuppgiftsbiträdet får endast överföra personuppgifter till tredjeland (utanför EU/EES) om Personuppgiftsansvarig på förhand skriftligen godkänt sådan överföring och den är förenlig med Tillämplig lag. Se närmare instruktioner för tredjelandsöverföring i **bilaga 1**.

4. Registrerades rättigheter

Personuppgiftsansvarig ansvarar för att informera registrerade om personuppgiftsbehandlingen och för att tillvarata registrerades rättigheter enligt Tillämplig lag. Personuppgiftsbiträdet ska vid behov och utan onödigt dröjsmål bistå Personuppgiftsansvarig i hanteringen av en registrerads begäran om exempelvis registerutdrag eller radering (registrerades rättigheter i enlighet med kapitel III i Dataskyddsförordningen).

Om Personuppgiftsbiträdet tar emot en begäran från registrerad om utövande av sina rättigheter eller tillhörande frågor, ska Personuppgiftsbiträdet hänvisa den registrerade till Personuppgiftsansvarig samt utan onödigt dröjsmål informera Personuppgiftsansvarig.

5. Sekretess och tystnadsplikt

Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska behandla personuppgifterna under sekretess/tystnadsplikt och inte avslöja eller göra personuppgifter tillgängliga för tredje part, om inte detta har godkänts i förväg av Personuppgiftsansvarig eller krävs enligt Tillämplig lag eller föreläggande från tillsynsmyndighet.

Personuppgiftsbiträdet ska säkerställa att endast sådan personal som måste ha tillgång till personuppgifter för att kunna fullgöra Personuppgiftsbiträdets skyldigheter enligt Personuppgiftsbiträdesavtalet får tillgång till sådana personuppgifter. Personuppgiftsbiträdet ska säkerställa att all sådan personal är bunden av sekretess/tystnadsplikt, antingen genom lag eller avtal, sådant avtal ska åtminstone motsvara det krav på sekretess/tystnadsplikt som följer av detta Personuppgiftsbiträdesavtal. Personuppgiftsbiträdet ska också säkerställa att personalen förstår innebörden av sekretess-/tystnadspliktsåtagandet.

Sekretess- och tystnadspliktsåtagandet gäller även under tid efter det att Personuppgiftsbiträdesavtalet i övrigt upphört att gälla.

6. Granskning, revision och kontroll

Personuppgiftsbiträdet ska bistå Personuppgiftsansvarig vid granskning inbegripet inspektion som tillsynsmyndighet kan komma att genomföra av Personuppgiftsansvarig. Personuppgiftsbiträdet ska utan dröjsmål informera Personuppgiftsansvarig om eventuella kontakter med tillsynsmyndighet. Personuppgiftsbiträdet får inte företräda Personuppgiftsansvarig eller på annat sätt agera för Personuppgiftsansvarigs räkning gentemot tillsynsmyndighet, eller annan tredje part, utan skriftligt medgivande från Personuppgiftsansvarig.

Personuppgiftsbiträdet ska ge Personuppgiftsansvarig tillgång till all information som krävs för att visa att behandling av personuppgifter uppfyller Tillämplig lag jämte de villkor som enligt detta Personuppgiftsbiträdesavtal gäller för personuppgiftsbehandling.

Personuppgiftsbiträdet förbinder sig att följa eventuella beslut från tillsynsmyndighet avseende behandlingen av personuppgifter för Personuppgiftsansvarigs räkning enligt detta Personuppgiftsbiträdesavtal.

Personuppgiftsansvarig får själv eller genom tredje part genomföra revision i skälig utsträckning eller på förekommen anledning gentemot Personuppgiftsbiträdet eller på annat sätt kontrollera att Personuppgiftsbiträdets behandling av personuppgifter följer detta Personuppgiftsbiträdesavtal. Vid sådan revision eller kontroll ska Personuppgiftsbiträdet ge Personuppgiftsansvarig den assistans som behövs för genomförande av den aktuella åtgärden.

För det fall att registrerade, tillsynsmyndighet eller annan tredje part begär information från någon av Parterna som på något sätt innefattar

behandling av personuppgifter enligt detta Personuppgiftsbiträdesavtal ska Parterna samverka och utbyta information i nödvändig utsträckning.

7. Personuppgiftsbiträdets anlitande av underbiträde

Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde (nedan ”Underbiträde”) för behandling av personuppgifter för Personuppgiftsansvarigs räkning utan ett i förväg inhämtat skriftligt godkännande från Personuppgiftsansvarig.

Om Personuppgiftsbiträdet anlitar ett Underbiträde för behandlingen av personuppgifter, ska Personuppgiftsbiträdet ålägga genom ett skriftligt avtal Underbiträdet motsvarande skyldigheter i fråga om dataskydd vid behandling av personuppgifter som gäller för Personuppgiftsbiträdet enligt detta Personuppgiftsbiträdesavtal. Om Underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd vid behandling av personuppgifter ska Personuppgiftsbiträdet vara fullt ansvarig gentemot Personuppgiftsansvarig för utförandet av det Underbiträdets skyldigheter.

I det fall Personuppgiftsbiträdet och Underbiträdet har ingått gällande Standardavtalsklausuler om tredjelandsöverföring har Standardavtalsklausulerna företräde i händelse av motstridig lydelse med detta Personuppgiftsbiträdesavtal.

De av Personuppgiftsansvarig godkända Underbiträdena framgår av instruktionen i **bilaga 1.**

Personuppgiftsansvarig eller av denne anlitad annan part har rätt till assistans från Personuppgiftsbiträdet vid revision och kontroll avseende behandling av personuppgifterna som utförs genom av denne anlitade Underbiträden.

8. Personuppgiftsincident

För det fall Personuppgiftsbiträdet misstänker alternativt upptäcker någon 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 (”Personuppgiftsincident”) ska Personuppgiftsbiträdet omedelbart undersöka Personuppgiftsincidenten och vidta lämpliga åtgärder för att läka Personuppgiftsincidenten och förhindra en upprepning.

Personuppgiftsbiträdet ska utan onödigt dröjsmål efter att ha fått vetskap om Personuppgiftsincidenten tillhandahålla Personuppgiftsansvarig en

beskrivning av Personuppgiftsincidenten och därefter löpande förse Personuppgiftsansvarig med information om Personuppgiftsincidenten.

Beskrivningen av Personuppgiftsincidenten ska åtminstone:

a) beskriva Personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgifter som berörs,

b) förmedla namnet på och kontaktuppgifterna till dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av Personuppgiftsincidenten, och

d) beskriva de åtgärder som Personuppgiftsbiträdet har vidtagit eller föreslagit för att åtgärda Personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

9. Ansvar

Vid ersättning för skada i samband med personuppgiftsbehandling som, genom fastställd dom, förlikning eller annat beslut, utgått till den registrerade på grund av överträdelse av bestämmelse i Tillämplig lag ska artikel 82 Dataskyddsförordningen tillämpas, jämte 7 kap. 1 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Vad gäller påförd administrativ sanktionsavgift enligt artikel 83 Dataskyddsförordningen och 6 kap. 2 och 3 §§ lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, ska den bäras av den av Parterna som påförts en sådan avgift.

Ansvar enligt denna punkt 9 st 1 och st 2 gäller före andra avtalsbestämmelser i Huvudavtalet om fördelning mellan Parterna av krav sinsemellan såvitt avser registrerads ersättning och sanktionsavgift.

Vad gäller skadeståndsansvar till följd av en parts avtalsbrott mot Personuppgiftsbiträdesavtalet gäller Huvudavtalets bestämmelser om påföljder.
Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

10. Ersättning för utförande av Personuppgiftsbiträdets uppdrag

Personuppgiftsbiträdet har inte rätt till ersättning under detta Personuppgiftsbiträdesavtal. Personuppgiftsbiträdets rätt till ersättning i övrigt är uteslutande reglerat i Huvudavtalet.

11. Personuppgiftsbiträdesavtalets giltighetstid

Detta Personuppgiftsbiträdesavtal träder ikraft på dagen för dess undertecknande och gäller så länge som Personuppgiftsbiträdet behandlar personuppgifter för Personuppgiftsansvarigs räkning som en del av åtagandet att leverera tjänst i enlighet med Huvudavtalet, eller vid den senare tidpunkt då personuppgifterna i sin helhet är raderade eller återlämnade enligt Personuppgiftsansvarigs instruktion.

12. Upphörande av behandling av personuppgifter

Vid upphörande av behandling av personuppgifter enligt Personuppgiftsbiträdesavtalet ska Personuppgiftbiträdet radera eller återlämna alla personuppgifter i enlighet med Personuppgiftsansvarigs instruktioner samt säkerställa att inga personuppgifter eller kopior därav är kvar i Personuppgiftsbiträdets besittning. Radering eller återlämnande ska utföras senast inom trettio (30) dagar från upphörandet av personuppgiftsbehandlingen.

Ovan utgör en precisering av eventuell reglering i Huvudavtalet avseende återlämning eller radering av data. I fall av motstridig lydelse avseende radering eller återlämning av data i Huvudavtalet och denna punkt 12 ska denna punkt ha företräde.

Om personuppgifterna återlämnas till Personuppgiftsansvarig ska det ske i ett öppet och standardiserat format som möjliggör återanvändning av personuppgifterna för liknande ändamål.

13. Ändringar och tillägg

Personuppgiftsansvarig får, i den mån så erfordras för att krav som följer av Tillämplig lag ska kunna tillgodoses, skriftligen ändra innehållet i detta Personuppgiftsbiträdesavtal. Sådan skriftlig ändring träder ikraft trettio (30) dagar efter det att meddelande härom översänts, om inte längre tidsfrist anges i meddelandet eller annan tidsfrist föranleds av Tillämplig lag.

Andra ändringar av och/eller tillägg till detta Personuppgiftsbiträdesavtal ska vara skriftliga och undertecknade av båda Parterna för att vara bindande.

14. Tvist

Tvist angående tolkning eller tillämpning av detta Personuppgiftsbiträdesavtal ska avgöras enligt svensk lag och av svensk allmän domstol.

15. Övrigt

Parterna ska inom ramen för Personuppgiftsbiträdesavtalet utse varsin kontaktperson.

Meddelanden inom ramen för Personuppgiftsbiträdesavtalet ska skickas till respektive parts kontaktperson för Personuppgiftsbiträdesavtalet.

Detta Personuppgiftsbiträdesavtal har upprättats i två originalexemplar, varav Parterna tagit var sitt.

Ort och datum	Ort och datum
Nämndens underskrift	Utförarens underskrift
Namnförtydligande	Namnförtydligande

Bilaga 1 - Instruktion till Personuppgiftsbiträdesavtal

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet följa gällande instruktioner vid behandling av personuppgifter för Personuppgiftsansvarigs räkning.

1. Ändamål för behandling av personuppgifter

Personuppgiftsbiträdet får behandla personuppgifter för Personuppgiftsansvarigs räkning för att tillhandahålla tjänsten/er i enlighet med Huvudavtalet. Personuppgiftsbiträdet ska bara behandla personuppgifterna för ändamålet att uppfylla sina åtaganden i enlighet med Huvudavtalet.

Här ska ni ange det specifika ändamålet med Personuppgiftsbiträdets behandling av personuppgifter d.v.s. syftet med den tjänst som ska utföras enligt Huvudavtalet, t.ex. tillhandahålla support och/eller applikations- och förvaltningsstöd:

2. Kategori av personuppgifter

Personuppgiftsbiträdet får för Personuppgiftsansvarigs räkning behandla följande kategorier av personuppgifter: *(fyll i)*

Med känsliga personuppgifter avses personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om fysisk persons sexualliv eller sexuella läggning.

Personuppgiftsbiträdet får behandla följande känsliga personuppgifter: *(fyll i)*

Vid behandling av känsliga och/eller särskilt skyddsvärda personuppgifter ska Personuppgiftsbiträdet införa sådana ytterligare åtgärder som krävs för skydd av sådana personuppgifter, se punkt 6.

3. Kategorier av registrerade

Ange de kategorier av registrerade vars personuppgifter kommer att behandlas är*: (fyll i)*

4. Plats för behandling

Personuppgiftsansvarig ska här beskriva
a) var personuppgifter får behandlas geografiskt, och
b) om tredjelandsöverföring är tillåten, beskriv det rättsliga stödet för den aktuella överföringen i enlighet med kap. V i Dataskyddsförordningen.

Med överföring av personuppgifter till tredjeland avses all personuppgiftsbehandling som kan komma att ske i ett tredjeland t. ex. då personuppgifter överförs till eller nås genom fjärråtkomst från tredjeland. Notera att ett bolags ägarförhållanden kan avgöra plats för behandling, detta som en följd av att exempelvis amerikansk s k problematisk lagstiftning kan möjliggöra för exempelvis amerikanska underrättelsemyndigheter att i vissa fall ställa krav på en utlämnandebegäran till ett amerikanskägt bolag, varvid en behandling kan komma att ske i USA.

Personuppgiftsbiträdet får behandla personuppgifterna på följande geografiska platser: *(fyll i, lista de länder i vilka personuppgifterna kommer att behandlas)*

Europeiska Unionen eller Europeiska Ekonomiska Samarbetsområdet (EES): *(fyll i)*

Tredjeland utanför EU/EES: *(fyll i)*

Innan tredjelandsöverföring får ske ska Parterna ha säkerställt att det finns ett rättsligt stöd för överföringen i form av exempelvis *adekvansbeslut* av EU-kommissionen om tillåten överföring, alternativt säkerställt ingående av *Standardavtalsklausuler kompletterat av genomförd riskanalys för tredjelandsöverföring* (s k Transfer Impact Assessment , TIA, i enlighet med Europeiska dataskyddsstyrelsens rekommendation[1]). Beskriv rättsligt stöd för varje tredjelandsöverföring som sker: *(fyll i)*

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021

Bilägg ingångna giltiga Standardavtalsklausuler mellan Personuppgiftsansvarig och Personuppgiftsbiträde, samt genomförd riskanalys för tredjelandsöverföring, TIA. Sker tredjelandsöverföringen mellan Personuppgiftsbiträde och dess Underbiträde är Personuppgiftsbiträdet ansvarig för ingåendet av Standardavtalsklausulerna med Underbiträdet och ska på begäran uppvisa dessa för Personuppgiftsansvarig.

5. Underbiträden

Följande Underbiträden hos Personuppgiftsbiträdet får behandla personuppgifter för Personuppgiftsansvarigs räkning:*(fyll i)*

Underbiträde	**Behandling sker i (land)**

6. Säkerhet; tekniska och organisatoriska åtgärder

De personuppgifter som behandlas av Personuppgiftsbiträdet ska skyddas på det sätt som anges i Personuppgiftsbiträdesavtalet (inklusive tillkommande skriftliga instruktioner från Personuppgiftsansvarig) jämte Tillämplig lag.

Artikel 32 p 1 Dataskyddsförordningen anger ”Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt
a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.”

Personuppgiftsbiträdet ska vidta och implementera följande beslutade tekniska och organisatoriska skyddsåtgärder enligt artikel 32 Dataskyddsförordningen: *(fyll i)*

Personuppgiftsbiträdet ska vid behov för att efterleva Tillämplig lag korrigera de implementerade tekniska och organisatoriska åtgärderna efter avstämning med Personuppgiftsansvarig. Notera att avtalsändringar regleras i punkt 13 Personuppgiftsbiträdesavtalet.

7. Återlämning eller radering av personuppgifter

Här anges specifika instruktioner om hur personuppgifter ska raderas eller återlämnas till Personuppgiftsansvarig*: (fyll i)*

8. Ytterligare instruktioner från Personuppgiftsansvarig

Personuppgiftsbiträdet ska se till att samtliga personer som behandlar personuppgifter enligt detta Personuppgiftsbiträdesavtal hos Personuppgiftsbiträdet har fått erforderlig utbildning om Tillämplig lag gällande personuppgiftsbehandling. Personuppgiftsbiträdet ska säkerställa att endast personer som behöver ha tillgång till personuppgifterna för utförandet av sitt arbete har tillgång till personuppgifterna.

Ange eventuella övriga tillkommande instruktioner för behandlingen, såsom exempelvis krav avseende gallring: *(fyll i)*

9. Varaktighet

Instruktionen gäller så länge som Personuppgiftsbiträdet behandlar personuppgifter för Personuppgiftsansvarigs räkning enligt Personuppgiftsbiträdesavtalet, inom ramen för utförandet av tjänsten enligt Huvudavtalet, eller till den tidpunkt då instruktionen ändras.

Personuppgiftsansvarig kan göra ändringar i och tillägg till denna Instruktion i enlighet med vad som följer av punkt 13 Personuppgiftsbiträdesavtalet.