

Bilaga 3 - Personuppgiftsbiträdesavtal

1. Parter

Personuppgiftsansvarig

Stockholms stad genom Hässelby-Vällingby stadsdelsförvaltning / Rinkeby-Kista stadsdelsförvaltning / Bromma stadsdelsförvaltning / Hägersten-Liljeholmen stadsdelsförvaltning / Norrmalms stadsdelsförvaltning / Spånga-Tensta stadsdelsförvaltning, nedan kallad Personuppgiftsansvarig. Org.nr. 212000-0142

Respektive stadsdel kommer ingå ett separat avtal med leverantören.

Personuppgiftsbiträde

[Personuppgiftsbiträdet], nedan kallad Personuppgiftsbiträde. Org.nr.

Gemensamt kallas dessa nedan Parterna.

Detta Personuppgiftsbiträdesavtal är en bilaga till Parternas Huvudavtal [datum] angående Vikariehanteringssystem, med Dnr. 2.2.1-524-2018.

2. Bakgrund och syfte

Enligt nuvarande bestämmelser i personuppgiftslagen (1998:204) (PuL) och kommande bestämmelser i Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (Dataskyddsförordningen, ”GDPR”), ska det finnas ett skriftligt avtal mellan Personuppgiftsansvarig och Personuppgiftsbiträde avseende den behandling av personuppgifter som Personuppgiftsbiträdet ska utföra för den Personuppgiftsansvariges räkning.

Detta Personuppgiftsbiträdesavtal mellan Parterna reglerar de skyldigheter som Personuppgiftsbiträdet har när personuppgifter behandlas för Personuppgiftsansvariges räkning. Syftet är att säkerställa att Personuppgiftsbiträdet behandlar personuppgifterna i enlighet med Personuppgiftsansvariges instruktioner och Tillämplig lag varmed avses PuL och Dataskyddsförordningen samt Datainspektionens och relevanta EU-organs föreskrifter, ställningstaganden och rekommendationer inom personuppgiftsområdet.

Närmare om Personuppgiftsbiträdes uppdrag framgår i ett mellan Parterna ingånget Huvudavtal till vilket detta Personuppgiftsbiträdesavtal utgör en bilaga. I händelse av motstridig lydelse mellan bestämmelserna i Personuppgiftsbiträdesavtalet och sådant Huvudavtal, ska Personuppgiftsbiträdesavtalet äga företräde om inte Parterna uttryckt annat.

3. Definitioner

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

4. Behandling av personuppgifter

Detta Personuppgiftsbiträdesavtal gäller för all behandling av personuppgifter under Huvudavtalet som utförs av Personuppgiftsbiträdet för Personuppgiftsansvarigs räkning.

Personuppgiftsbiträdet och personer som agerar för Personuppgiftsbiträdets räkning får behandla personuppgifter endast i enlighet med Personuppgiftsbiträdesavtalet och de ytterligare skriftliga instruktioner som Personuppgiftsansvarig från tid till annan lämnar.

Personuppgiftsbiträdet ska bara behandla personuppgifterna för ändamålet att uppfylla sina åtaganden i enlighet med Huvudavtalet. Om Personuppgiftsbiträdet saknar instruktioner eller är osäker på ändamålet med behandlingen som bedöms vara nödvändigt för att genomföra en viss uppgift som innebär eller kan innebära behandling av Personuppgifter, ska Personuppgiftsbiträdet, utan dröjsmål, informera Personuppgiftsansvarig om detta och därefter invänta vidare instruktioner från Personuppgiftsansvarig.

Personuppgiftsbiträdet åtar sig, vad avser behandlingen av personuppgifter, att följa tillämplig lag. Personuppgiftsbiträdet ska själv hålla sig informerad om tillämplig lag.

Personuppgiftsbiträdets åtaganden att följa tillämplig lag ska i alla avseenden tolkas i enlighet med beskaffenheten på Personuppgiftsbiträdets tillhandahållna tjänster och innebär normalt sett att Personuppgiftsbiträdet inte själv samlar in personuppgifter eller använder personuppgifterna för annat bruk än för uppfyllelse av avtalad leverans enligt Huvudavtalet. Personuppgiftsbiträdet ska i vilket fall inte, utan föreläggande från relevant myndighet eller tvingande lagstiftning:

a) samla in eller lämna ut personuppgifter från eller till någon tredje part om inte annat skriftligen överenskommit,

- b) ändra metod för behandling,
- c) kopiera eller återskapa personuppgifter,
- d) eller på något annat sätt behandla personuppgifter för andra ändamål än de som anges i Huvudavtalet.

Personuppgiftsbiträdet ska vidta alla åtgärder som krävs enligt artikel 32 i Dataskyddsförordningen.

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

Personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att tillse att skyldigheterna enligt artiklarna 32-36 i Dataskyddsförordningen fullgörs, med beaktande av typen av behandling och den information som Personuppgiftsbiträdet har att tillgå.

5. Register över personuppgiftsbehandling

Personuppgiftsbiträdet eller dennes företrädare ska föra ett register över alla kategorier av behandling av personuppgifter som utförs för den Personuppgiftsansvariges räkning. Av registret ska åtminstone framgå

- a) namn och kontaktuppgifter för Personuppgiftsbiträdet eller de av denne anlitate personuppgiftsbiträdena, för den Personuppgiftsansvarige och för den Personuppgiftsansvariges eller Personuppgiftsbiträdets företrädare samt dataskyddsombudet,
- b) de kategorier av behandling av personuppgifter som Personuppgiftsbiträdet utför för den Personuppgiftsansvarige,
- c) om överföringar av personuppgifter sker till tredjeland eller en internationell organisation, jämte uppgift om vilket tredjeland eller internationell organisation det är fråga om,
- d) dokumentation över vilka lämpliga säkerhetsåtgärder som vidtagits, om överföring sker till sådant tredjeland som inte omfattas av beslut enligt tillämpliga bestämmelser om adekvat skyddsnivå eller lämpliga skyddsåtgärder samt
- e) om möjligt, en allmän beskrivning av vidtagna tekniska och organisatoriska säkerhetsåtgärder som ska vidtas enligt tillämpliga rättsliga krav.

Personuppgiftsbiträdet ska på begäran av den Personuppgiftsansvarige eller behörig tillsynsmyndighet tillhandahålla ett registerutdrag med innehåll enligt ovan.

Om en Registrerad under utövandet av sina rättigheter begär ett registerutdrag avseende behandlingen av dennes personuppgifter, ska Personuppgiftsbiträdet på begäran av den Registrerade eller den Personuppgiftsansvarige tillhandahålla registerutdrag avseende sådan behandling med innehåll och på sätt enligt tillämpliga rättsliga krav.

6. Säkerhet och sekretess

Personuppgiftsbiträdet ska implementera tekniska och organisatoriska skyddsåtgärder i enlighet med tillämplig lag eller i annat fall upprätta lämpliga tekniska och organisatoriska åtgärder i syfte att skydda personuppgifter mot obehörig eller olovlig förstörelse eller oavsiktlig förlust av, förändring av, otillåtet yppande av eller tillgång till personuppgifter, i huvudsak när behandlingen innefattar spridning av uppgifter över nätverk och mot all annan olovlig form av behandling. Vid bedömning av lämplig säkerhetsnivå ska särskilt hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstörelse, förlust eller ändring eller till obehörigt röjande eller obehörig åtkomst till personuppgifter.

Personuppgiftsbiträdet ska säkerställa att behörighetsstyrningen är korrekt och att konfidentialitet iakttas.

Personuppgiftsbiträdet ska tillse att samtliga anställda, konsulter och övriga som Personuppgiftsbiträdet svarar för och som behandlar personuppgifterna är bundna av ett ändamålsenligt 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 om hur de får behandla dem i enlighet med instruktioner från Personuppgiftsansvarig.

Sekretessåtagandet gäller även under tid efter det att Personuppgiftsbiträdesavtalet i övrigt upphört att gälla, dock längst till och med sådan tidpunkt som gäller enligt särskilt tillämpliga rättsliga krav.

Personuppgiftsbiträdet får inte utan (i) Personuppgiftsansvariges skriftliga samtycke i förväg, och (ii) att säkerställa att sådan överföring sker i överensstämmelse med tillämplig lagstiftning, överföra personuppgifter till land utanför EU/EES-området eller till land som inte omfattas av undantagen till förbud mot överföring till tredje land enligt Tillämplig lag. Detta förbud omfattar även teknisk support, underhåll och liknande tjänster.

7. Revision och begäran av information

Personuppgiftsbiträdet ska utan dröjsmål informera Personuppgiftsansvarig om eventuella kontakter med Datainspektionen eller annan myndighet som rör eller kan vara av betydelse för behandling av personuppgifter. Personuppgiftsbiträdet äger ej rätt att företräda Personuppgiftsansvarig eller på annat sätt agera för Personuppgiftsansvarigs räkning gentemot Datainspektionen eller annan tredje man utan skriftligt medgivande från Personuppgiftsansvarig.

Personuppgiftsansvarig äger rätt att själv eller genom tredje man genomföra revision gentemot Personuppgiftsbiträdet eller på annat sätt kontrollera att Personuppgiftsbitrådets 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. Personuppgiftsbiträdet äger rätt till ersättning från Personuppgiftsansvarige för styrkta skäligen direkta kostnader som Personuppgiftsbiträdet åsamkas till följd av sådan revision eller kontroll.

Personuppgiftsbiträdet ska ge den Personuppgiftsansvarige tillgång till all information som krävs för att visa att behandling av personuppgifter uppfyller tillämpliga rättsliga krav jämte de villkor som enligt detta Personuppgiftsbiträdesavtal gäller för personuppgiftsbehandling.

För det fall att Registrerade, Datainspektionen eller annan tredje man begär information från någon av Parterna som på något sätt innefattar personuppgifter ska Parterna samverka och utbyta information i nödvändig utsträckning.

Personuppgiftsbiträdet får inte lämna ut personuppgifter eller någon annan information om behandlingen av personuppgifter utan skriftligt medgivande från Personuppgiftsansvarige, såvida inte föreläggande från relevant myndighet eller tvingande lagstiftning finns.

8. Personuppgiftsbitrådets anlitan av annan

Personuppgiftsbiträdet får inte anlita annat personuppgiftsbiträde för behandling av personuppgifter för den Personuppgiftsansvariges räkning utan skriftligt godkännande från den Personuppgiftsansvarige.

Om Personuppgiftsbiträdet anlitar ett annat personuppgiftsbiträde för behandlingen av personuppgifter, ska Personuppgiftsbiträdet ålägga det andra personuppgiftsbiträdet samma skyldigheter i fråga om dataskydd som gäller för Personuppgiftsbiträdet enligt detta Personuppgiftsbiträdesavtal. Personuppgiftsbiträdet ska vidare tillse att sådant personuppgiftsbiträde respekterar och följer de villkor som gäller i detta Personuppgiftsbiträdesavtal och i övrigt följer de skyldigheter som följer av tillämpliga rättsliga krav.

Om Personuppgiftsbiträdet i enlighet med detta Personuppgiftsbiträdesavtal anlitar personuppgiftsbiträden, ska Personuppgiftsbiträdet tillse att dennes avtal med dessa utformas så att personuppgiftsbiträdena blir bundna av detta Personuppgiftsbiträdesavtal och de i avtalet angivna kraven jämte tillämpliga rättsliga krav. Om det andra personuppgiftsbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska Personuppgiftsbiträdet vara fullt ansvarig gentemot den Personuppgiftsansvarige för utförandet av det andra personuppgiftsbiträdets skyldigheter.

De anlitade personuppgiftsbiträdena ska vid var tid vara kända av Personuppgiftsbiträdet och vid anmodan från den Personuppgiftsansvarige redovisas till denne. Den Personuppgiftsansvarige eller av denne anlitad annan part har rätt till assistans från Personuppgiftsbiträdet vid kontroll eller revision avseende behandling av personuppgifterna som utförs genom av denne anlitade personuppgiftsbiträden.

9. Personuppgiftsincident

För det fall Personuppgiftsbiträdet misstänker alternativt upptäcker någon 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 en upprepning.

Personuppgiftsbiträdet ska utan onödigt dröjsmål efter att ha fått vetskap om incidenten tillhandahålla Personuppgiftsansvarig en beskrivning av incidenten och därefter löpande förse Personuppgiftsansvarig med information om incidenten i takt med att information blir tillgängligt för Personuppgiftsbiträdet.

Beskrivningen av incidenten 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 den Personuppgiftsansvariga har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Personuppgiftsbiträdet ska informera Personuppgiftsansvarige om Personuppgiftsbiträdet får kännedom om att personuppgifter behandlas 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 det att behandlingen utförs vara Personuppgiftsansvarig behjälplig vid en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

10. Skadelöshetsförbindelse

För det fall Registrerade, Datainspektionen eller annan tredje man väcker krav mot någon av Parterna avseende Personuppgiftsbiträdets eller av denne anlitat personuppgiftsbiträdes behandling av personuppgifter ska Personuppgiftsbiträdet hålla Personuppgiftsansvarig skadelös från alla krav som orsakats av Personuppgiftsbiträdets eller av denne anlitat personuppgiftsbiträdes överträdelse av Personuppgiftsbiträdesavtalet. Oaktat vad som anges i Huvudavtalet och dess Bilagor gäller denna förpliktelse före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser behandling av personuppgifter.

11. Ersättning

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

12. Personuppgiftsbiträdesavtalets giltighetstid

Detta Personuppgiftsbiträdesavtal träder ikraft på dagen för dess undertecknande och gäller så länge som Personuppgiftsbiträdet behandlar personuppgifter under Huvudavtalet.

13. Upphörande av behandling av personuppgifter

Vid upphörande av behandling av personuppgifter enligt Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet radera alla personuppgifter eller lämna tillbaka dem till Personuppgiftsansvarige på sådant sätt som angivits av Personuppgiftsansvarige och i enlighet med Personuppgiftsansvariges instruktioner samt säkerställa att inga personuppgifter eller kopior därav är kvar i Personuppgiftsbiträdes besittning.

14. Ändringar och tillägg

Personuppgiftsansvarig får, i den mån så erfordras för att krav som följer av Tillämplig lag ska kunna tillgodoses, ändra innehållet i detta

Personuppgiftsbiträdesavtal. Sådan ändring träder ikraft senast trettio (30) dagar efter att Personuppgiftsansvarig översänt meddelandet om ändring till Personuppgiftsbiträdet. För det fall Personuppgiftsbiträdet inte accepterar den aktuella ändringen, äger Personuppgiftsansvarig rätt att omedelbart säga upp alla avtal med Personuppgiftsbiträdet enligt vilka Personuppgiftsbiträdet ska behandla personuppgifter.

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

15. Tillämplig lag och tvist

Tvist avseende tolkning eller tillämpning av Personuppgiftsbiträdesavtalet ska slutligt avgöras enligt vad som anges rörande tvist i Huvudavtalet.

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

För Personuppgiftsansvarige

För Personuppgiftsbiträdet

Ort och datum

Ort och datum

Nämndens/bolagets underskrift

Leverantörens underskrift

Namnförtydligande

Namnförtydligande