Avtal

MELLAN PERSONUPPGIFTSANSVARIG OCH PERSONUPPGIFTSBITRÄDE

1. Personuppgiftsbiträdesavtalets syfte

Detta Personuppgiftsbiträdesavtal syftar till att uppfylla stadgandet i Artikel 28 i Europaparlamentets och rådets förordning (EU) 2016/679 (dataskyddsförordningen), som föreskriver att det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning.

2. Definitioner

I den mån dataskyddsförordningen innehåller begrepp som motsvarar de som används i detta avtal ska sådana begrepp tolkas och tillämpas i enlighet med dataskyddsförordningen.

Detta avtal har motsvarande definitioner som återfinns i Artikel 4 dataskyddsförordningen, vilket bland annat innebär att:

a) med **personuppgiftsansvarig** avses den som ensamt eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter,

b) med **personuppgiftsbiträde** avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning,

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

d) med **personuppgifter** avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

3. Innehåll

Personuppgiftsansvarig är Göteborgs Stad och personuppgiftsbiträde är utföraren.

Mellan den Personuppgiftsansvarige och Personuppgiftsbiträdet ska det finnas ett avtal avseende tillhandahållande av tjänster enligt förfrågningsunderlaget (”Tjänsteavtalet”).

Tjänsteavtalet är det avtal som reglerar vad Personuppgiftsbiträdet ska utföra för den Personuppgiftsansvariges räkning. Personuppgiftsbiträdet behandlar personuppgifter i den omfattning som krävs för att uppfylla åtagandena enligt Tjänsteavtalet.

4. Ansvar och instruktion

Den Personuppgiftsansvarige har ansvar för all behandling av avtalade personuppgifter i enlighet med dataskyddsförordningen.

Personuppgiftsbiträdet åtar sig att enbart behandla avtalade personuppgifter i enlighet med Tjänsteavtalet och den Personuppgiftsansvariges vid var tid meddelade instruktioner. Personuppgiftsbiträdet får endast behandla personuppgifter på dokumenterade instruktioner från Personuppgiftsansvarige.

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

Personuppgiftsbiträdet får 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 överenskommits;
b) ändra metod för behandling;
c) kopiera eller återskapa personuppgifter;

eller på något annat sätt behandla personuppgifter för andra ändamål än de som anges i Tjänsteavtalet.

Personuppgiftsbiträdet får inte utan Personuppgiftsansvariges skriftliga samtycke i förväg, överföra några personuppgifter till land utanför EES-området eller till land som inte omfattas av undantagen till förbud mot överföring till tredje land enligt dataskyddsförordningen. Personuppgiftsbiträdet ska vid sådan överföring säkerställa att det sker i överensstämmelse med tillämplig lagstiftning. Förbudet omfattar även teknisk support, underhåll och liknande tjänster.

För det fall Personuppgiftsbiträdet misstänker eller 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 (i) undersöka incidenten och vidta lämpliga åtgärder för att läka incidenten och förhindra en upprepning, och (ii) tillhandahålla Personuppgiftsansvarig en beskrivning av incidenten.

Beskrivning 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 personuppgiftsposter som berörs,
c) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
e) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
g) beskriva de åtgärder som den personuppgiftsansvarige 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 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.

5. 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:

a) de tekniska möjligheter som finns,
b) vad det skulle kosta att genomföra åtgärderna,
c) de särskilda risker som finns med behandlingen av personuppgifterna och
d) hur känsliga de behandlade personuppgifterna är.

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

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 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.

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet 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 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 personuppgifterna i enlighet med instruktioner från Personuppgiftsansvarig.

6. Revision och besök

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.

I de fall registrerade personer, Datainspektionen eller annan tredje man begär information från Personuppgiftsansvarige eller Personuppgiftsbiträdet rörande behandlingen av personuppgifter ska parterna samverka och utbyta information i nödvändig utsträckning. Ingen part får lämna ut personuppgifter eller information om behandlingen av personuppgifter utan medgivande i förväg från motparten utom för det fall föreläggande finns därom från relevant myndighet eller om part 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.

7. Underbiträden

I den mån Personuppgiftsbiträdet anlitar underbiträden, ska dessa godkännas av Personuppgiftsansvarig om inte annat skriftligen avtalats mellan parterna.

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 avtal.

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.

Personuppgiftsbiträdet ska informera den personuppgiftsansvarige om eventuella planer på att anlita nya underbiträden eller ersätta underbiträden, så att den Personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar. För det fall det finns rimligt fog för invändningen har Personuppgiftsansvarige rätt att med bindande verkan motsätta sig anlitandet av visst nytt underbiträde.

8. Skadelöshet

Personuppgiftsbiträdet ska hålla Personuppgiftsansvarig skadeslöst i händelse av att Personuppgiftsansvarig åsamkas skada som är hänförlig till Personuppgiftsbiträdets behandling av personuppgifter i strid med instruktion från Personuppgiftsansvarig eller Tjänsteavtalet.

9. Upphörande av behandling av personuppgifter

Personuppgiftsbiträdet ska beroende på vad Personuppgiftsansvarig väljer, radera eller återlämna all data som innehåller personuppgifter på samtliga media som den är fixerad på, efter uppdraget har avslutats och radera befintliga kopior.

10. Överlåtelse

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

11. Tvist och tillämplig lag

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