

Personuppgiftsbiträdesavtal

Projektnamn

Projekt-ID

Ordernummer/Produktnummer

Innehållsförteckning

Personuppgiftsbiträdesavtal.....	3
1. Bakgrund och syfte	3
2. Personuppgiftsansvariges ansvar.....	3
3. Personuppgiftsbitrådets åtaganden	4
3.1. Sekretess.....	4
3.2. Personuppgiftsincident	5
4. Ändringar och tillägg i personuppgiftsbiträdesavtal.....	5
5. Ansvar gentemot tredje man	5
6. Lagval och tvistelösning	5
7. Avtalstid och upphörande av behandling.....	5
Bilaga 1. Instruktion.....	7
Bilaga 2. Tekniska och organisatoriska åtgärder för MONA inom SCB (personuppgiftsbitrådet)	9

Personuppgiftsbiträdesavtal

Avtal enligt 28.3, Allmänna dataskyddsförordningen EU 2016/679

Personuppgiftsansvarig	Personuppgiftsbiträde
	Statistiska centralbyrån (SCB)
Organisationsnummer	Organisationsnummer
	202100-0837
Adress	Adress
	701 89 ÖREBRO

1. Bakgrund och syfte

Detta avtal reglerar personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning. Avtalet är utformat med beaktande av kraven i EU:s dataskyddsförordning EU 2016/679. Termer som används i detta avtal har den innebörd som återfinns i artikel 4 i dataskyddsförordningen.

Personuppgiftsbiträdet, SCB, tillhandahåller användarytor för projektet samt personliga ytor (My Documents) för den personuppgiftsansvariges räkning i samband med utlämnande av uppgifter i MONA (Microdata Online Access) för ovan nämnda projekt. Mottagaren, den personuppgiftsansvarige, bestämmer ändamålet med behandlingen samt vilka kategorier av registrerade personer som ska behandlas. Personuppgiftsbiträdet har inte tillgång till uppgifterna efter utlämnandet. Den behandling som sker av uppgifterna genom tillhandahållandet av användarytor samt My Documents är endast att se som ett led i teknisk bearbetning eller lagring enligt 2 kap. 13 § tryckfrihetsförordningen. Personuppgiftsbiträdet kommer lagra uppgifterna inom EU/EES tills den personuppgiftsansvarige väljer att lämna avtalet.

2. Personuppgiftsansvariges ansvar

Den personuppgiftsansvarige åtar sig att vid behov komplettera den av SCB förifyllda instruktionen, se bilaga 1. Detta för att personuppgiftsbiträdet ska kunna fullgöra sitt uppdrag enligt detta avtal.

3. Personuppgiftsbitrådets åtaganden

Personuppgiftsbitrådets uppgifter och ansvar framgår av artikel 28 i dataskyddsförordningen. För SCB, som personuppgiftsbiträde, innebär det bland annat följande:

Personuppgiftsbitrådet får inte behandla, utnyttja eller sprida personuppgifter på något annat sätt, för andra ändamål eller andra instruktioner än vad som framgår av dataskyddsförordningen och detta personuppgiftsbiträdesavtal.

För att skydda behandlingen av personuppgifter ska personuppgiftsbitrådet åta sig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder, se bilaga 2, i enlighet med dataskyddslagstiftningens krav. Personuppgiftsbitrådet ska möjliggöra samt bidra till uppföljning samt bistå den personuppgiftsansvarige vid konsekvensbedömningar och förhandssamråd.

Personuppgiftsbitrådet ska, med beaktande av behandlingens art, genom lämpliga tekniska och organisatoriska åtgärder bistå den personuppgiftsansvarige att fullgöra sina skyldigheter att tillgodose den registrerades rättigheter.

Personuppgiftsbitrådet ska omedelbart informera personuppgiftsansvarige om personuppgiftsbitrådet anser att instruktionen strider mot förordningen eller annan dataskyddsbestämmelse.

Personuppgiftsbitrådet förbinder sig att inte överföra personuppgifter till tredje land.

Den personuppgiftsansvarige ska informeras samt ges möjlighet att göra invändningar innan personuppgiftsbitrådet anlitar ett annat personuppgiftsbiträde (underbiträde).

3.1. Sekretess

Personuppgiftsbitrådet garanterar att anställda, underbiträden och konsulter har åtagit sig att iaktta konfidentialitet eller omfattas av laglig tystnadsplikt.

3.2. Personuppgiftsincident

Vid en personuppgiftsincident ska personuppgiftsbiträdet utan onödigt dröjsmål underrätta personuppgiftsansvarig om händelsen samt upprätta en skriftlig beskrivning av personuppgiftsincidenten.

Personuppgiftsbiträdet åtar sig att på begäran av den personuppgiftsansvariga anmäla en i MONA-systemet inträffad personuppgiftsincident till Integritetsskyddsmyndigheten inom 72 timmar.

Personuppgiftsbiträdet kan inte, enligt dataskyddsförordningen, överta det juridiska ansvaret.

4. Ändringar och tillägg i personuppgiftsbiträdesavtal

Ändringar och tillägg av detta avtal ska, för att vara giltiga, vara skriftliga och undertecknade av båda parter.

5. Ansvar gentemot tredje man

Om registrerad eller tredje man riktar krav mot den personuppgiftsansvarige, på grund av personuppgiftsbitrådets behandling av personuppgifter, ska personuppgiftsbiträdet hålla den personuppgiftsansvarige skadelös för sådana krav som följer av att personuppgiftsbiträdet inte följt instruktioner eller detta avtal.

6. Lagval och tvistelösning

För detta avtal gäller svensk rätt.

7. Avtalstid och upphörande av behandling

Detta avtal gäller från undertecknandet och så länge som personuppgiftsbiträdet behandlar den personuppgiftsansvariges personuppgifter. Detta avtal ersätter eventuella tidigare tecknade personuppgiftsbiträdesavtal.

När personuppgiftsbitrådets uppdrag enligt avtal har slutförts ska samtliga personuppgifter, inklusive befintliga kopior, raderas på ett sådant sätt att de inte kan återskapas om inte annat följer av lag. Personuppgiftsbiträdet ska skriftligen bekräfta att så skett.

Personuppgiftsbiträdesavtalet har upprättats i två (2) exemplar, varav parterna har tagit var sitt.

På personuppgiftsansvariges
vägnar:

På personuppgiftsbitrådets
vägnar:

Ort och datum

Ort och datum

Befattning

Befattning

Underskrift

Underskrift

Namnförtydligande

Namnförtydligande

Bilaga 1. Instruktion

Utöver vad som framgår av detta avtal ska personuppgiftsbiträdet följa nedanstående instruktioner.

Ändamål	<i>Syftet med de personuppgifter som personuppgiftsbiträdet kommer behandla.</i>
Kategorier av registrerade personer	<i>Vilka kategorier av registrerade personer ska behandlas? Ex. kommuninvånare, pensionärer, anställda inom en viss verksamhet.</i>
Personuppgifter	<i>Vilken typ av personuppgifter behandlas? Inkludera även uppgifter från andra registerhållare om det ingår.</i>
Känsliga personuppgifter enligt Dataskyddsförordningen	<i>Vilka ev. känsliga personuppgifter kommer behandlas?</i>
Behandling	<i>Hur kommer personuppgifterna att behandlas?</i> Uppgifterna i MONA som omfattas av detta personuppgiftsbiträdesavtal ska endast göras tillgängliga för bearbetning och analys för de som personuppgiftsansvarig utser. Användarna ska kunna ta ut resultat i form av statistik, grafer eller annat.

Särskilda instruktioner angående behandling	<i>Ska personuppgiftsbiträdet särskilt beakta något vid behandlingen?</i>
--	---

Bilaga 2. Tekniska och organisatoriska åtgärder för MONA inom SCB (personuppgiftsbiträdet)

Följande tekniska och organisatoriska åtgärder ska följas av SCB:

Åtkomst. Personuppgiftsbiträdet har inte rätt att ta del av uppgifterna utan den personuppgiftsansvariges godkännande. Endast utpekade personer hos personuppgiftsbiträdet kan få åtkomst till personuppgifterna för att uppfylla sin roll som personuppgiftsbiträde. Endast på uppdrag av personuppgiftsansvarig kan personuppgiftsbiträdet tilldelas åtkomst till uppgifterna utanför personuppgiftsbitrådets organisation.

Tillträdeskontroll. För att säkerställa att enbart behörig personal får tillträde till utrymmen där det finns IT-utrustning ska det finnas rutiner för tillträdeskontroll.

Datasäkerhet. Datasystem ska vara skyddade mot obehörig åtkomst, t.ex. användning, påverkan och stöld.

Säkerhetskopiering. Uppgifter ska regelbundet säkerhetskopieras och uppgifter som kopieras/flyttas till sekundär lagringsmedia (backup) ska vara krypterade om så överenskommit. Kopiorna ska förvaras väl avskilt och förvaras på ett betryggande sätt. Personuppgiftsbiträdet ska ha rutiner för test av återläsning.

Fysisk säkerhet. Datorresurser ska fysiskt vara skyddade från åtkomst utifrån genom lås, larm och andra fysiska säkerhetsåtgärder. Det ska vidare finnas brandskyddsteknik i lokalerna.

Överföring och kommunikation. Personuppgifter då de överförs via öppna nät ska skyddas mot förstöring, ändring och förvanskning. Vidare ska personuppgifterna skyddas mot obehörig åtkomst och anslutningar ska skyddas mot obehörig trafik.

Loggning. Personuppgiftsbiträdet ska upprätthålla loggning.

Användning. Personuppgiftsbiträdet ska vid behov sammanställa information om användningen av uppgifterna.

Skydd mot skadlig kod. Datasystem ska vara skyddad mot skadegörande programvara såsom virus, maskar och trojaner.

Utplåning. När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre ska användas för sitt ändamål ska personuppgifterna raderas på sådant sätt att de inte kan återskapas.

Reparation och service. När reparation och service av datorutrustning, vilken används för att lagra personuppgifter, utförs av annan än personuppgiftsbiträdet, ska avtal som reglerar säkerhet och sekretess träffas med serviceföretaget. Vid servicebesök ska service ske under personuppgiftsbitrådets uppsikt. Är detta inte möjligt ska lagringsmedier som innehåller personuppgifter avlägsnas. Service via fjärrstyrd datorkommunikation får endast ske via säker anslutning och efter säker elektronisk identifiering av den som utför service. Servicepersonal ska ges åtkomst i systemet endast vid servicetillfället. Finns separat kommunikationsingång för service ska den vara stängd när service inte pågår.