

**PERSONUPPGIFTSBITRÄDES-
AVTAL**

Ärendenr:
NV-08385-18

Avtal om behandling av personuppgifter

1. Parter

Personuppgiftsansvarig

Organisation:	
Adress:	
Postnummer och ort:	
Organisationsnummer:	
Kontaktperson:	
E-post:	
Telefonnummer:	

Personuppgiftsbiträde

Organisation:	Naturvårdsverket
Adress:	Naturvårdsverket
Postnummer och ort:	106 48 Stockholm
Organisationsnummer:	2021001975
Kontaktperson:	Anna Otmalm
E-post:	anna.otmalm@naturvardsverket.se
Telefonnummer:	010-698 15 48

2. Definitioner

Detta personuppgiftsbiträdesavtal har motsvarande definitioner som återfinns i artikel 4 i dataskyddsförordningen¹, vilket bl.a. innebär följande.

¹ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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).

Med *personuppgifter* avses varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med *behandling* avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättning av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Med *pseudonymisering* avses behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Personuppgiftsincident avser en 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 och i övrigt behandlas.

3. Innehåll och syfte

Detta avtal har upprättats för att uppfylla de krav som framgår av dataskyddsförordningen, andra gällande författningar på området och etablerad standard samt att uppgifterna inte blir tillgängliga för obehöriga.

Mellan Naturvårdsverket och personuppgiftsansvarig har ett avtal avseende användning av sammanhållet tjänsteerbjudande för underrättelse om medelstora förbränningsanläggningar upprättats ("Användaravtalet"). Användaravtalet reglerar vad personuppgiftsbiträdet ska utföra för personuppgiftsansvarigs räkning. Personuppgiftsbiträdet behandlar personuppgifter i den omfattning som krävs för att uppfylla åtagandena enligt Användaravtalet.

4. Personuppgiftsbiträdesavtalets avtalshandlingar

Personuppgiftsbiträdesavtalet består av detta dokument samt Bilaga 1 - Instruktioner för behandling av personuppgifter och Bilaga 2 – Inbyggt dataskydd.

5. Behandlingar som omfattas av personuppgiftsbiträdesavtalet

5.1 Preciserade instruktioner till personuppgiftsbiträdet avseende dennes behandling av personuppgifter inom ramen för detta personuppgiftsbiträdesavtal framgår av bilaga 1.

5.2 Åtgärderna för inbyggt dataskydd och dataskydd som standard ska genomföras av parterna i enlighet med instruktionerna i bilaga 2.

5.3 Parterna ska säkerställa att vid var tid gällande instruktioner framgår av bilaga 1 och 2.

6. Behandling av personuppgifter

6.1 Personuppgiftsbiträdet åtar sig att behandla personuppgifter i enlighet med dataskyddsförordningen, detta personuppgiftsbiträdesavtal samt i enlighet med vid var tid gällande instruktioner från personuppgiftsansvarig hänförliga till detta personuppgiftsbiträdesavtal.

6.2 Personuppgiftsansvarig bestämmer ensam ändamålet med och medlen för den behandling av personuppgifter som personuppgiftsbiträdet utför för personuppgiftsansvarigs räkning.

6.3 Personuppgiftsbiträdet får inte behandla personuppgifter för något annat ändamål eller på något annat sätt än vad som vid varje behandlingstillfälle är nödvändigt för att uppfylla sina åtaganden enligt personuppgiftsbiträdesavtalet och Användaravtalet.

7. Personuppgiftsbitrådets skyldigheter

7.1 Personuppgiftsbiträdet garanterar att denne besitter nödvändig kapacitet och förmåga att fullgöra sina skyldigheter enligt detta personuppgiftsbiträdesavtal och gällande dataskyddslagstiftning, samt att denne löpande vidtar sådana lämpliga tekniska och organisatoriska åtgärder som krävs för att säkerställa att den registrerades rättigheter skyddas. Personuppgiftsbiträdet ska följa föreskrifter och rekommendationer från Datainspektionen och andra myndigheter som har en styrande inverkan på personuppgiftsansvarig verksamhet och som ger vägledning vad gäller informationssäkerhet.

7.2 Personuppgiftsbiträdet ska på personuppgiftsansvarigs begäran visa att de skyldigheter som framgår av detta personuppgiftsbiträdesavtal och gällande dataskyddsregler uppfyllts.

7.3 För det fall att personuppgiftsbiträdet saknar instruktioner som personuppgiftsbiträdet bedömer är nödvändiga för att genomföra uppdraget ska personuppgiftsbiträdet utan dröjsmål, informera personuppgiftsansvarig om sin inställning och invänta instruktioner från personuppgiftsansvarig.

7.4 Personuppgiftsbiträdet ska utan dröjsmål informera personuppgiftsansvarig om eventuella kontakter från Datainspektionen som rör eller kan vara av betydelse för behandling av personuppgifterna. Personuppgiftsbiträdet har inte rätt att företräda personuppgiftsansvarig eller agera för myndighetens räkning gentemot Datainspektionen eller annan tredje man.

7.5 För det fall att registrerad, Datainspektionen eller annan tredje man begär information från personuppgiftsbiträdet som rör behandlade personuppgifter ska personuppgiftsbiträdet hänvisa till personuppgiftsansvarig. Personuppgiftsansvarig och personuppgiftsbiträdet ska därefter komma överens om lämpligt tillvägagångsätt för utgivande av efterfrågad information.

7.6 Personuppgiftsbiträdet ska på personuppgiftsansvarigs begäran bistå personuppgiftsansvarig att fullgöra sina skyldigheter enligt gällande dataskyddsregler (artikel 32–36), såsom att utföra konsekvensbedömningar avseende dataskydd och genomföra förhandssamråd med Datainspektionen.

7.7 Personuppgiftsbiträdet ska vid behov bistå personuppgiftsansvarig att tillmötesgå en begäran om rättelse, blockering eller utplåning av personuppgifter som framställts av den registrerade.

7.8 Personuppgiftsbiträdet ska underrätta personuppgiftsansvarig vid en personuppgiftsincident. Se punkt 10.

7.9 Personuppgiftsansvarig har rätt att ta del av de uppgifter som registreras i tjänstens logg. Uppgifter i loggen får endast användas av personuppgiftsansvarig för vad som krävs för upprätthållande av tjänstens funktionalitet och kvalitet.

7.10 Personuppgiftsansvarig har rätt att själv eller genom tredje man kontrollera att personuppgiftsbiträdet följer vad som anges i detta personuppgiftsbiträdesavtal. Personuppgiftsbiträdet ska då kostnadsfritt lämna personuppgiftsansvarig den hjälp och tillhandahålla den dokumentation som erfordras för detta.

7.11 Personuppgiftsbiträdet har inte rätt till särskild ersättning för åtaganden enligt personuppgiftsbiträdesavtalet.

8. Sekretess och tystnadsplikt

8.1 Behandling av personuppgifter ska, i förekommande fall, ske i enlighet med angiven sekretessklausul i Användaravtalet. Tillämpliga bestämmelser i offentlighet- och sekretesslagen (2009:400) ska följas.

8.2 Personuppgiftsbiträdet ansvarar för att berörda personer (inklusive personer hos eventuellt underbiträde) informeras om och iakttar gällande sekretess. Personuppgiftsbiträdet ska se till att berörda personer omfattas av tystnadsplikt avseende de personuppgifter som behandlas.

8.3 Personuppgiftsbiträdet, dennes personal eller eventuellt underbiträde får inte lämna ut några uppgifter till tredje man utan att först ha inhämtat skriftligt medgivande från personuppgiftsansvarig. Detta gäller under förutsättning att handlingarna inte är allmänna handlingar hos personuppgiftsbiträdet. Personuppgiftsbiträdet har skyldighet att följa gällande författningar.

9. Underbiträden

9.1 Personuppgiftsbiträdet får ett allmänt skriftligt förhandstillstånd att anlita underbiträde. Personuppgiftsbiträdet redovisar anlitade underbiträden i Bilaga 1 till detta personuppgiftsbiträdesavtal.

Personuppgiftsbiträdet ska skriftligen informera personuppgiftsansvarig om eventuella planer på att anlita nytt underbiträde eller ersätta underbiträde.

Personuppgiftsansvarig har rätt att inom 30 dagar invända mot anlitande av nytt underbiträde om personuppgiftsansvarig har sakliga skäl härför. Sakliga skäl är om det nya underbiträdet inte kan förväntas leva upp till de krav på personuppgiftsbehandling som följer av tillämplig dataskyddslagstiftning.

Personuppgiftsbiträdet ska genom skriftligt avtal ålägga underbiträdet samma skyldigheter som följer av detta personuppgiftsbiträdesavtal.

9.2 Om underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska personuppgiftsbiträdet vara fullt ansvarigt gentemot personuppgiftsansvarig för utförandet av underbiträdets skyldigheter.

9.3 För att personuppgiftsansvarig ska kunna uppfylla sina lagstadgade skyldigheter som personuppgiftsansvarig, ska samtliga underbiträden vara kända av och redovisade för personuppgiftsansvarig. Personuppgiftsansvarig måste även ha kännedom om i vilket land behandlingen äger rum.

10. Underrättelse i händelse av personuppgiftsincident

10.1 Personuppgiftsbiträdet ska efter att ha fått vetskap om en personuppgiftsincident (se punkt 2 och punkt 7.8) utan onödigt dröjsmål underrätta personuppgiftsansvarig, via e-post

En sådan underrättelse ska åtminstone innehålla nedanstående information som får lämnas i omgångar.

a) En beskrivning av 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,

b) Namn och kontaktuppgifter till personuppgiftsbiträdets dataskyddsombud eller andra kontaktuppgifter där mer information kan erhållas,

c) En beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten och

d) En beskrivning av 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.

Om personuppgiftsansvarig eller Datainspektionen så begär ska personuppgiftsbiträdet informera den registrerade om en personuppgiftsincident på så sätt som följer av dataskyddsförordningen.

11. Överföring av personuppgifter till tredjeland

11.1 Personuppgiftsbiträdet äger inte rätt att överföra personuppgifter till tredjeland eller en internationell organisation utan att personuppgiftsansvarig har lämnat sitt skriftliga samtycke i förväg till en sådan överföring.

11.2 En överföring till tredjeland förutsätter under alla förhållanden, d.v.s. även för det fall personuppgiftsansvarig lämnat sitt skriftliga samtycke, att personuppgiftsbiträdet uppfyller de krav och åtgärder som följer av dataskyddsförordningen vad avser tredjelandsöverföring.

12. Skada och ansvar

Ansvar för skada regleras i enlighet med artikel 82 i dataskyddsförordningen.

13. Ändringar och tillägg

13.1 Ändringar och tillägg till detta personuppgiftsbiträdesavtal ska göras skriftligen och undertecknas av behöriga företrädare för båda parter för att vara giltiga.

13.2 Om tjänstens innehåll ändras t.ex. genom nya funktioner som innebär att nya sätt att behandla personuppgifter tillkommer, ska personuppgiftsansvarig omgående underrättas om förändringarna.

14. Åtgärder vid avslut

14.1 Vid personuppgiftsbiträdesavtalets upphörande ska personuppgifterna antingen återföras till personuppgiftsansvarig, i ett läsbart och allmänt använt format, eller raderas. Om annat inte meddelas av personuppgiftsansvarig ska personuppgifterna återföras till personuppgiftsansvarig och därefter raderas hos personuppgiftsbiträdet så snart de inte längre behövs för att fullgöra uppdraget från personuppgiftsansvarig. På begäran ska personuppgiftsbiträdet lämna ett skriftligt besked om vilka åtgärder som vidtagits med personuppgifterna i samband med att behandlingen slutförts.

14.2 För det fall att personuppgiftsbiträdet på grund av författning är skyldigt att behålla personuppgifter även efter det att detta personuppgiftsbiträdesavtal har upphört att gälla får dessa personuppgifter endast användas för det ändamål som

framgår av den författning som föranleder att personuppgifterna behålls. Personuppgiftsansvarig ska informeras om detta och grunderna härför.

15. Överlåtelse av avtal

15.1 Personuppgiftsbiträdet äger inte rätt att helt eller delvis överlåta sina åtaganden enligt detta personuppgiftsbiträdesavtal till annan utan skriftligt medgivande från personuppgiftsansvarig.

16. Avtalstid, uppsägning och avtalsuppföljning

16.1 Personuppgiftsbiträdesavtalet träder i kraft när det har undertecknats av parterna. Avtalet gäller så länge som personuppgiftsbiträdet behandlar personuppgifter för personuppgiftsansvarigs räkning.

16.2 Regler om uppsägning finns i Användaravtalet.

16.3 Personuppgiftsbiträdesavtalet ska följas upp i samband med den ordinarie uppföljningen av Användaravtalet.

17. Tillämplig lag och tvist

17.1 Parternas rättigheter och skyldigheter enligt detta personuppgiftsbiträdesavtal bestäms av svensk rätt.

17.2 Tvist angående tolkning eller tillämpning av detta personuppgiftsbiträdesavtal ska avgöras enligt svensk lag och föras vid allmän svensk domstol.

Detta personuppgiftsbiträdesavtal har upprättats i två (2) likalydande exemplar av vilka parterna tagit var sitt.

Ort och datum

Ort och datum

Stockholm

Personuppgiftsansvarig

Personuppgiftsbiträde

Namnteckning

Namnteckning

Namnförtydligande

Anna Otmalm

Namnförtydligande

Titel

Avdelningschef

Titel

Bilaga 1 – Instruktioner för behandling av personuppgifter

Parterna har nedan konkretiserat vad som ingår i behandlingen enligt personuppgiftsbiträdesavtalet.

I. Ändamålet med behandlingen

Ändamålet med behandling av personuppgifter är att personuppgiftsbiträdet, i egenskap av teknisk tjänsteleverantör, ska kunna tillhandahålla och vidareutveckla ett sammanhållet tjänsteerbjudande för underrättelse av medelstora förbränningsanläggningar ("Tjänsten").

II. Kategorier av registrerade

Tjänsten behandlar personuppgifter relaterade till uppgiftslämnare (verksamhetsutövare eller betrodd företrädare) och tillsynsmyndighet.

III. Vilken typ av personuppgifter behandlas

De personuppgifter som behandlas är följande:

Personuppgifter relaterade till kontaktperson/företrädare för verksamhetsutövare

- eidasPersonIdentifier (*ID-nyckel för individ med utländsk e-legitimation*)
- Personnummer
- Namn
- Telefonnummer
- E-postadress
- Roll i företaget (*kan vara firmatecknare, intern företrädare, extern företrädare*)
- Engagemang i företaget (*vid hämtning från Bolagsverket via SSBTGU*)
- Organisationsnummer (*är personuppgift om företagsformen är enskild näringsidkare*)
- Företagsnamn
- Fastighetsbeteckning
- AnläggningsID för anläggning
- Namn på anläggning
- Besöksadress för anläggning
- Koordinater för anläggning

Personuppgifter relaterade till kontaktperson för tillsynsmyndighet

- E-postadress (*om individspecifik e-postadress uppgivits*)
- Namn
- Telefonnummer

IV. Särskilda kategorier av personuppgifter och särskilt integritetskänsliga uppgifter (i förekommande fall)

Inga särskilda kategorier av personuppgifter eller integritetskänsliga uppgifter får behandlas.

V. Behandling

Behandling av personuppgifter kommer endast ske för teknisk bearbetning och teknisk lagring för tillsynsmyndighetens räkning.

VI. Särskilda instruktioner rörande behandlingen

Utöver vad som framgår av användaravtalet ges följande instruktioner.

De roller som behandlar personuppgifter ska begränsas till teknisksupport och teknikadministratör.

Dessa roller utför följande:

- För att kunna ge uppgiftslämnare support i ett serviceskede och tillsynsmyndigheten support vid mottagning av överförda uppgifter behöver teknisksupportrollen tillgång till personuppgifter i produktionsmiljö.
- För att kunna förvalta, vidareutveckla och säkerställa driften av Tjänsten behöver teknikadministratörsrollen tillgång till personuppgifter för att kunna leveranstesta, acceptanstesta samt felsöka Tjänsten i produktionsmiljö.

VII. Behandling av underbiträden i tredjeland (i förekommande fall)

Personuppgiftsbiträdet förbinder sig att inte överföra, lagra eller på annat vis behandla Personuppgifter tillhörande Personuppgiftsansvarig utanför EU/EES utan Personuppgiftsansvarigs godkännande.

VIII. Åtgärder vid avslut

Se punkt 14 i personuppgiftsbiträdesavtalet.

IX. Godkända underbiträden

Organisation	Typ av behandling	Plats för behandling (land)
CGI Sverige AB	Drift och viss utveckling av Tjänsten	Sverige
Consid AB	Utveckling och förvaltning av Tjänsten	Sverige

Bilaga 2 – Inbyggt dataskydd

Parterna ansvarar var för sig och i samråd med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt risker, att vidta lämpliga tekniska och organisatoriska åtgärder utformade för ett inbyggt dataskydd och dataskydd som standard i enlighet med gällande dataskyddslagstiftning.

Parterna har vidtagit följande tekniska och organisatoriska åtgärder för inbyggt dataskydd.

Säkerhetsåtgärder

- Säker inloggning av uppgiftslämnare sker i e-tjänsten med eLegitimation, som uppfyller kraven i eIDAS-förordningen.
- Uppgiftslämnare med skyddad identitet (person med sekretessmarkering i folkbokföringsregistret) skyddas genom att förhindras lämna in uppgifter via e-tjänsten.
- Säker hämtning av folkbokföringsuppgifter till eget utrymme sker genom att e-tjänsten ansluter till Skatteverkets bastjänst NAVET, utifrån fastställt regelverk för användning av tjänsten. Säker kommunikation sker via en SSL-krypterad kommunikationskanal.
- Säker hämtning av företagsuppgifter till eget utrymme sker genom att e-tjänsten ansluter till Bolagsverkets sammansatta bastjänst, SSBTGU, utifrån fastställt regelverk för användning av tjänsten. Säker kommunikation sker via en SSL-krypterad kommunikationskanal.
- Säker hämtning av tidigare inlämnade uppgifter till eget utrymme sker genom att e-tjänsten ansluter till Tjänstens sammansatta bastjänst SSBTSNA. Säker kommunikation sker via en SSL-krypterad kommunikationskanal med IP-låsning.
- Säker överföring av information till tillsynsmyndigheten sker med e-post via en SSL-krypterad kommunikationskanal.
- De olika verksamhetsutövarnas information hålls separerad med hjälp av behörighetsstyrning.
- De olika tillsynsmyndigheternas information hålls separerad med hjälp av behörighetsstyrning.
- För att möjliggöra felsökning vid meddelandeöverföring mellan e-tjänsten och bastjänsterna genomförs loggning.
- Uppgifter (och Tjänsten) skyddas från otillbörlig påverkan genom skalskydd.
- För att förhindra oavsiktlig förvanskning/radering av uppgifter säkerhetskopieras alla uppgifter som behandlas i Tjänsten.
- För att säkra Tjänstens tillgänglighet driftövervakas Tjänsten.