PERSONUPPGIFTSBITRÄDESAVTAL

Version: 2018-05-12

Detta avtal reglerar förhållandet mellan ”Personuppgiftsansvarig” och ”Personuppgifts-biträdet”.

Med “Personuppgiftsbiträdet” avses Web IT Solutions AB (”Leverantören”) med avseende på de tjänster som har avtalats med Kunden.

Med ”Personuppgiftsansvarig” avses Kunden.

För frågor kring Web IT Solutions behandling av personuppgifter och aktuella gällande villkor hänvisas till företagets webbplats.

1 Allmänt

1.1 Detta Personuppgiftsbiträdesavtal utgör en integrerad del av avtalet som ingåtts mellan Leverantören och Kunden (”Avtalet”).

1.2 Leverantören kommer vid fullföljandet av Avtalet att behandla Personuppgifter för Kundens räkning såsom Kundens personuppgiftsbiträde. Kunden är personuppgiftsansvarig för behandlingen av personuppgifterna.

1.3 Om någon annan tillsammans med Kunden är personuppgiftsansvarig för de aktuella personuppgifterna ska Kunden skriftligt informera Leverantören om detta.

1.4 Syftet med detta personuppgiftsbiträdesavtal är att Kunden och Leverantören ska uppfylla vid var tid gällande krav på personuppgiftsbiträdesavtal och förpliktelser enligt nedanstående Dataskyddsregler samt att säkerställa ett adekvat skydd för personlig integritet och grundläggande rättigheter för enskilda i samband med överföring av Personuppgifter från Kunden till Leverantören inom ramen för de tjänster Leverantören utför åt Kunden under Avtalet.

2. Definitioner

Dataskyddsregler	avser vid var tid gällande lag eller förordning som ska tillämpas på behandling av Personuppgifter vilket innefattar men inte är begränsat till personuppgiftslagen (1998:204) och från den 25 maj 2018 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”) vilken ersätter personuppgiftslagen 1998:204); samt Tillsynsmyndighets bindande beslut och föreskrifter samt tillkommande lokal anpassning och reglering avseende dataskydd.

Kunden	avser den part som anges ovan, i den mån Kunden ingår detta avtal för andra tjänstemottagares räkning i enlighet med Avtalet ska dock definitionen ”Kund” i tillämpliga delar även avse sådana tjänstemottagare om inte annat uttryckligen framgår av detta Personuppgiftsbiträdesavtal.
Leverantören	avser den part som anges ovan.
Personuppgifter	avser 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 lokaliseringsuppgift eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet, som Leverantören behandlar för Kundens räkning under detta Personuppgiftsbiträdesavtal.
Registrerad	avser den fysiska person som en Personuppgift avser.
Tillsynsmyndighet	avser den eller de tillsynsmyndigheter som har behörighet att bedriva tillsyn över behandling av Personuppgifter eller anses vara berörd tillsynsmyndighet enligt Dataskyddsregler, t.ex. Datainspektionen.
Underbiträde	avser den som behandlar Personuppgifter som underleverantör åt Leverantören.

2.1 Eventuella övriga definitioner med stor begynnelsebokstav, eller som i övrigt kan relateras till behandling av personuppgifter, som används i detta Personuppgiftsbiträdesavtal ska, om inget annat uttryckligen anges, ha den innebörd och betydelse som framgår i första hand av Dataskyddsregler och annars av Avtalet om inte omständigheterna uppenbarligen talar för annan tolkningsordning.

3. Ansvar och instruktion

3.1 Kunden är personuppgiftsansvarig för samtliga Personuppgifter som Leverantören behandlar för Kundens räkning under Avtalet. Kunden ansvarar därmed för att gällande dataskyddsregler följs. Kunden har skyldighet att informera Leverantören om eventuell förändring i Kunds verksamhet som gör att Leverantören behöver vidta någon form av åtgärd eller förändrad rutin gällande innehållet i Dataskyddsregler. Utöver de krav som gäller direkt för Leverantören enligt Dataskyddsregler ska Leverantören vara skyldig att följa vid var tid gällande krav i Dataskyddsregler samt gällande rekommendationer från Tillsynsmyndighet. Kunden ska även löpande informera Leverantören om tredje parts, däribland Tillsynsmyndighets och Registrerads, åtgärder med anledning av behandlingen.

3.2 Leverantören och den eller de personer som arbetar under Leverantörens ledning ska endast behandla Personuppgifter i enlighet med Kundens dokumenterade instruktioner och inte för några andra ändamål än dem som Leverantören anlitats för och som anges i detta person-

uppgiftsbiträdesavtal. De särskilda instruktioner som gäller vid Personuppgiftsbiträdesavtalets ingående framgår av Bilaga 1, utöver de särskilda instruktionerna skall detta Personuppgiftsbiträdesavtal och Avtalet i övrigt anses utgöra Kundens samtliga instruktioner till Leverantören avseende behandling av Personuppgifter. Kunden ska omedelbart informera Leverantören om förändringar vilka påverkar Leverantörens skyldigheter enligt detta Personuppgiftsbiträdesavtal.

3.3 Behandling får även ske om sådan behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som Leverantören eller Underbiträde omfattas av. Om behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som Leverantören eller Underbiträde omfattas av ska Leverantören eller Underbiträdet informera Kunden om det rättsliga kravet innan behandlingen, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt sådan rätt.

3.4 Leverantören har rätt att under Personuppgiftsbiträdesavtalets giltighetstid och därefter lagra och behandla data som härrör från Kunden i aggregerat eller anonymiserat format, d.v.s. data som inte innehåller Personuppgifter.

4 Säkerhet m.m.

4.1 Leverantören ska vidta de åtgärder som krävs för att uppfylla Artikel 32 i Dataskyddsförordningen. Leverantören ska därvid säkerställa en säkerhetsnivå som är lämplig i förhållande till risken som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som behandlas.

4.2 Leverantören ska även bistå Kunden med att se till att skyldigheterna enligt Artiklarna 32-36 i Dataskyddsförordningen fullgörs, med beaktande av typen av behandling och den information som Leverantören har att tillgå. Leverantören skall säkerställa att personer med behörighet att behandla Personuppgifterna antingen omfattas av en lagstadgad tystnadsplikt eller har åtagit sig det i ett bindande avtal. Tystnadsplikten skall gälla även efter det att detta Personuppgiftsbiträdesavtal upphört att gälla. Åtkomst till Personuppgifterna skall begränsas till sådana personer som behöver dem för att kunna utföra sina arbetsuppgifter.

5. Utlämnande av Personuppgifter och information

5.1 Om det till Leverantören kommer in en begäran från Registrerad, Tillsynsmyndighet eller annan tredje man om att få ta del av uppgifter som Leverantören behandlar för Kundens räkning ska Leverantören utan dröjsmål vidarebefordra begäran till Kunden. Leverantören, eller den som arbetar under Leverantörens ledning, får inte lämna ut Personuppgifter eller annan information om behandlingen av Personuppgifter utan uttrycklig instruktion om detta från Kunden om inte sådan skyldighet föreligger enligt gällande Dataskyddsregler.

5.2 Leverantören ska, med tanke på behandlingens art, hjälpa Kunden genom tekniska och organisatoriska åtgärder, i den mån det är möjligt, så att Kunden kan fullgöra sin skyldighet att svara på begäran från den Registrerade vid den Registrerades utövande av sina rättigheter enligt Dataskyddsregler i enlighet med kapitel III i Dataskyddsförordningen.

5.3 Kunden ska utge separat ersättning till Leverantören för Leverantörens arbete med anledning av sina åtaganden enligt denna punkt 5 i enlighet med Leverantörens vid var tid gällande prislista.

6 Kontakt med Tillsynsmyndigheten

Leverantören ska informera Kunden om eventuella kontakter från Tillsynsmyndigheten som rör Behandling av Personuppgifter.

7 Underbiträden

7.1 Personuppgifter får behandlas av ett Underbiträde under förutsättning att Leverantören på Kundens vägnar ingår ett skriftligt avtal eller annan rättsakt enligt unionsrätten där Underbiträdet åläggs motsvarande skyldigheter i fråga om dataskydd som Leverantören åläggs enligt detta Personuppgiftsbiträdesavtal.

7.2 Leverantören åtar sig att informera Kunden om eventuella planer på att anlita nya Underbiträden eller ersätta Underbiträden. Kunden har rätt att invända mot sådana förändringar. Sådan invändning får endast hänföra sig till objektiva grunder hänförliga till exempelvis säkerheten av behandlingen enligt Personuppgiftsbiträdesavtalet. Om Kunden gör en sådan befogad invändning och Leverantören inte accepterar att byta ut aktuellt Underbiträde har Leverantören rätt till extra ersättning av Kunden för de kostnader som Leverantören drabbas av p.g.a. aktuellt Underbiträde inte kan användas. Leverantören har även rätt att säga upp Avtalet och/eller detta Personuppgiftsbiträdesavtal helt eller delvis, t.ex. vad avser viss tilläggstjänst med trettio (30) dagars uppsägningstid

7.3 Leverantören är särskilt ansvarig för att tillse att Artiklarna 28.2 och 28.4 i Dataskyddsförordningen beaktas vid anlitande av Underbiträden och att tillse att sådant Underbiträde ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i Dataskyddsförordningen.

7.4 Leverantören ska på begäran från Kunden tillhandahålla Kunden (och om så begärs, Kundens kunder som är personuppgiftsansvariga) en korrekt och uppdaterad lista om vilka Underbiträden som anlitats av Leverantören för behandlingen av Personuppgifter, kontaktuppgifter till dessa samt den geografiska placeringen för sådan behandling.

8 Rätt till insyn

8.1 Leverantören ska ge Kunden tillgång till all information som krävs för att visa att de skyldigheter som följer av Artikel 28 i Dataskyddsförordningen har fullgjorts inom skälig tid efter sådan begäran framställts av Kunden till Leverantören. Detta medför bland annat att Kunden, i egenskap av personuppgiftsansvarig, har rätt att vidta nödvändiga åtgärder för att verifiera att Leverantören kan fullfölja sina åtaganden enligt detta Personuppgiftsbiträdesavtal och att Leverantören faktiskt har vidtagit åtgärder för att säkerställa detta.

8.2 Leverantören ska även möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av Kunden eller av en annan oberoende revisor.

9 Överföring av Personuppgifter utanför EU/EES

9.1 Överföring av Personuppgifter av Leverantören eller av Underbiträde till en plats utanför EES-området (s.k. tredje land) får vidtas förutsatt att vid var tid gällande krav för sådan överföring enligt Dataskyddsregler uppfylls. Leverantören ska vid sådan överföring tillämpa och i förhållande till Underbiträde i tredje land för Kundens räkning ingå avtal där Underbiträdet åläggs att tillämpa, EU:s standardklausuler (2010/87/EU) eller de standardklausuler som ersätter dessa efter eventuellt beslut av EU-kommissionen och/eller EU-domstolen.

10 Sekretess

10.1 Leverantören ska säkerställa att personer med behörighet att behandla Personuppgifterna antingen omfattas av en lagstadgad tystnadsplikt eller har åtagit sig det i ett bindande avtal. Tystnadsplikten ska gälla även efter det att detta Personuppgiftsbiträdesavtal upphört att gälla. Åtkomst till Personuppgifterna skall begränsas till sådana personer som behöver dem för att kunna utföra sina arbetsuppgifter.

10.2 Åtagandet i punkt 10.1 ovan gäller inte information som Leverantören föreläggs utge till myndighet eller enligt Dataskyddsregler eller annan lagstadgad skyldighet. Sekretessåtagandet gäller under Avtalets giltighetstid och därefter.

11 Dataportabilitet

11.1 Leverantören ska tillse att Kunden kan uppfylla eventuell skyldighet att möjliggöra dataportabilitet avseende Personuppgifter som Leverantören behandlar för Kundens räkning.

12 Ersättning

12.1 Leverantören ska ha rätt till full ersättning från Kunden för samtligt arbete och samtliga kostnader som uppstår till följd av fullgörande av punkterna 8, 11 och 15.1 som beror på instruktioner för behandling av personuppgifter som Kunden ger Leverantören och som går utöver vad som framgår av Bilaga 1 eller de funktioner och den säkerhetsnivå som följer av de tjänster som Leverantören normalt erbjuder sina kunder, t.ex. vad gäller Leverantörens servertjänster och sådant som kräver att Leverantören behöver göra specialanpassningar på beställning av Kunden. Leverantören ska även ha rätt till ersättning för sitt arbete med anledning av sina åtaganden enligt punkt 5. Samtligt arbete som Leverantören har rätt till ersättning för enligt denna punkt ska ersättas i enlighet med Leverantörens vid var tid gällande prislista. Kostnadsersättning ska ersättas med Leverantörens faktiska havda kostnader.

13 Ansvar

13.1 Om Leverantören, den som arbetar under Leverantörens ledning eller av Leverantören anlitat Underbiträde behandlar Personuppgifter i strid med detta Personuppgiftsbiträdesavtal eller de lagenliga anvisningar som Kunden har lämnat, ska Leverantören med beaktande av de ansvarsbegränsningar som följer av Avtalet, ersätta Kunden för den direkta skada som Kund har orsakats på grund av den felaktiga behandlingen, inklusive skadestånd och administrativa sanktionsavgifter som Kunden behövt erlägga till tredje man. Oaktat ansvarsbegränsning enligt Avtalet ska Leverantörens ansvar enligt denna punkt 13.1 alltid vara begränsat till ett belopp motsvarande de avgifter som Kunden erlagt till Leverantören under Avtalet under en period om tolv (12) månader innan skadan uppstod.

13.2 Om Kunden, den som arbetar under Kundens ledning eller av Kunden anlitad tredje part orsakar Leverantören skada som beror på otydliga, bristfälliga eller otillåtna instruktioner från Kunden, bristfällig information från Kunden om vilka kategorier av uppgifter som behandlas (t.ex. om känsliga Personuppgifter behandlas utan att Kunden informerat Leverantören om detta) eller som annars beror på brott mot detta Personuppgiftsbiträdesavtal, ska Kunden ersätta Leverantören för sådan skada, inklusive skadestånd och administrativa sanktionsavgifter som Leverantören behövt erlägga till tredje man.

13.3 Leverantörens ersättningsskyldigheter avseende krav och skador enligt denna punkt 13 gäller under förutsättning att i) Kunden utan onödigt dröjsmål skriftligen underrättar

Leverantören om krav som framställts mot Kunden; och ii) Kunden låter Leverantören kontrollera försvaret av kravet och ensam fatta beslut om eventuell förlikning.

14 Avtalstid och åtgärder vid upphörande

14.1 Personuppgiftsbiträdesavtalet gäller från dess undertecknande och så länge som Leverantören behandlar Personuppgifter för Kundens räkning

.

15 Ändringar i Personuppgiftsbiträdesavtalet

15.1 Om Dataskyddsregler ändras under tiden för Personuppgiftsbiträdesavtalet, eller om Tillsynsmyndighet utfärdar riktlinjer, beslut eller föreskrifter kring tillämpningen av Dataskyddsregler som föranleder att detta Personuppgiftsbiträdesavtal inte uppfyller de krav som ställs på ett personuppgiftsbiträdesavtal ska parterna i god anda diskutera nödvändiga förändringar av detta Personuppgiftsbiträdesavtal för att tillgodose sådana nya eller tillkommande krav. Sådan ändring träder ikraft enligt parternas skriftliga överenskommelse därom, eller annars senast inom sådan tidsperiod som anges i Dataskyddsregler, Tillsynsmyndighets riktlinjer, beslut eller föreskrifter. Leverantören har rätt till skälig ersättning för eventuellt arbete, kostnader och utgifter som sådana ändringar föranleder.

15.2 Övriga ändringar av och tillägg till detta Personuppgiftsbiträdesavtal ska för att vara bindande upprättas skriftligen och vara behörigen undertecknade av Parterna.

16 Övrigt

16.1 I övrigt ska vad som sägs i Avtalet äga tillämpning även för Leverantörens behandling av Personuppgifter och åtagandena under detta Personuppgiftsbiträdesavtal. Vid oenighet mellan bestämmelserna i Avtalet och detta Personuppgiftsbiträdesavtal ska dock bestämmelserna i Personuppgiftsbiträdesavtalet äga företräde i förhållande till all behandling av Personuppgifter och inget i Avtalet ska anses begränsa eller ändra åtaganden i detta Personuppgiftsbiträdesavtal i den mån att detta skulle medföra att någon part inte uppfyller kraven enligt Dataskyddsregler.

16.2 Svensk lag ska under alla omständigheter tillämpas på detta Personuppgiftsbiträdesavtal. Tvister som uppstår i anledning av detta Personuppgiftsbiträdesavtal ska lösas i enlighet med tvistlösningsbestämmelsen i Avtalet.

Bilaga 1 – Hantering av personuppgifter

Hantering av personuppgifter
Följande instruktioner gäller för behandling av Personuppgifter av Leverantören, både i egenskap av personuppgiftsansvarig och i egenskap av personuppgiftsbiträde i enlighet med personuppgiftsbiträdesavtalet. Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Leverantören följa nedanstående instruktioner

Ändamål	Behandlingen av personuppgifter sker hos Leverantören såsom personuppgiftsansvarig, och i vissa fall där Leverantören är personuppgiftsbiträde, i syfte att leverera, utveckla, förvalta, felsöka, underhålla och administrera Leverantörens tjänster till och avtalsförhållande med Kunden.
Kategorier av Personuppgifter	I egenskap av personuppgiftsansvarig behandlas uppgifter som t.ex. namn, e-post, personnummer, adress, telefonnummer och liknande kontaktinformation till kund. Leverantören behandlar också till viss del användarnamn och IP-adresser. I egenskap av personuppgiftsbiträde kan ytterligare kategorier förekomma (regleras då av personuppgiftsansvarige).
Kategorier av Registrerade	I egenskap av personuppgiftsansvarig behandlas information om kunder, leverantörer och partners till Leverantören. I egenskap av personuppgiftsbiträde kan ytterligare kategorier förekomma (regleras då av personuppgiftsansvarige).
Gallringstid	Personuppgifter som lagras direkt i våra system gallras eller anonymiseras inom skälig tid efter att Kund helt avslutat sin Tjänst och vårt åtagande enligt Avtalet upphört, eller om Kund valt att aktivt kräva borttagning av sina uppgifter. Undantag är data som har lagkrav att sparas längre (t.ex finansiell information för Skatteverket eller bokföringsinformation) och dessa sparas då så länge vi har lagkrav på att spara informationen. Information som lagras indirekt på våra tjänster, som t.ex. backuper av Kunds data, loggar eller liknande sparas mellan 7 dagar och 12 månader beroende på tjänst.
Praktisk hantering	Insamling av uppgifter i egenskap av personuppgiftsansvarig sker vid Avtalsskrivning mellan Kund och Leverantör och då också godkännande av villkor. Kundens information används för att identifiera Kund (både manuellt och automatiskt) för t.ex. utskick av fakturor och vid kommunikation med support. Vid beställning av tredjepartstjänster som t.ex. domäner/SSL-certifikat skickas den information som krävs till tredje part. IP-adresser och användarnamn behandlas också i form av loggning, monitorering & backup. Behandlingar som utförs från Leverantören i rollen personuppgiftsbiträde utgörs normalt av exempelvis loggning, felsökning, monitorering, backup och kundtjänst/support.

Tekniska och organisatoriska säkerhetsåtgärder
Nedan listas de åtgärder som tas från Leverantören i egenskap av personuppgiftsansvarig och Personuppgiftsbiträde för att säkerställa att personuppgifterna behandlas på ett säkert vis.

Privacy-by-design	Utvecklingsprocesser och mjukvara från Leverantör tas fram med rutiner/processer som utgår från ett inbyggt dataskydd.
Fysiskt skydd	Utrymmen där personuppgifter förvaras, så som serverhallar & kontor, ska skyddas genom lämpliga tillträdeskontroller för att säkerställa att endast behörig personal får tillträde.
Skydd mot skadlig kod	Relevanta system ska vara skyddade mot virus, trojaner och andra former av digitala intrång.
Begränsning av access	Inloggningar och accesser är rollbaserade och individbaserade, och grunden är att personal och system inte har mer access än nödvändigt för att utföra uppgiften.
Backup	Leverantören har backuper både på system där denne behandlar personuppgifter i egenskap av personuppgiftsansvarig, och där våra kunder behandlar personuppgifter.
Loggning	Leverantören har fullgod loggning kring access och ändring av personuppgifter.
Kryptering	All kommunikation över internet mellan system som hanterar personuppgifter sker krypterat.
Riskbedömning	Leverantören utför löpande riskanalyser kring våra system och våra tjänster.
Processer och rutiner	Leverantören har tydliga processer och rutiner för de olika typer av behandlingar som utförs.
Systemregister	Leverantören har fullgoda hjälpmedel för att få en bra kontroll på de system, enheter och organisationer som behandlar personuppgifter.