**PERSONUPPGIFTSBITRÄDESAVTAL**

1. PARTER

Detta personuppgiftsbiträdesavtal (”**Biträdesavtalet**”) har denna dag ingåtts mellan

MELLAN

* 1. [NAMN], [ORG NR], [ADRESS], (nedan kallade "**Vårdgivaren**”)   
       
     OCH

1.2 [NAMN], [ORG NR], [ADRESS], (nedan kallad "**Biträdet**”).

Vårdgivaren och Biträdet benämns i det följande även var för sig som ”**Part**” eller gemensamt som ”**Parterna**”.

2. SYFTET MED PERSONUPPGIFTSBEHANDLINGEN

2.1 Vårdgivaren bedriver sådan verksamhet för vilken Behandling av Personuppgifter utgör en naturlig del. Parterna har träffat ett avtal (”**Huvudavtalet**”) varigenom Biträdet har åtagit sig att för Vårdgivarens räkning tillhandahålla journalföring och journalföringssystem som en molntjänst. Vid utförandet av tjänsterna enligt Huvudavtalet kommer Biträdet att Behandla Personuppgifter för Vårdgivarens räkning. Biträdet kommer därmed vid de aktuella tjänsterna enligt Huvudavtalet att få tillgång till Personuppgifter som Vårdgivaren är personuppgiftsansvarig för enligt Tillämplig Dataskyddslagstiftning. Detta innebär att Vårdgivaren är Personuppgiftsansvarig och att Biträdet kommer att agera som Vårdgivarens Personuppgiftsbiträde vid Behandlingen av Personuppgifter.

2.2 Tillämplig Dataskyddslagstiftning uppställer krav på att skriftligt avtal (personuppgiftsbiträdesavtal) träffas mellan den som är Personuppgiftsansvarig och den som är Personuppgiftsbiträde. Detta Biträdesavtal ska reglera Biträdets Behandling av Personuppgifter för Vårdgivarens räkning. Biträdesavtalet ska säkerställa att de Personuppgifter som omfattas av Biträdets Behandling hanteras i enlighet med de krav som följer av lagstiftning och etablerad standard samt att uppgifterna inte blir tillgängliga för obehöriga.

2.3 Detta Biträdesavtal utgör bilaga till av Parterna träffat Huvudavtal. I händelse av motstridigheter mellan Biträdesavtalet och Huvudavtalet ska vad som anges i detta Biträdesavtal äga företräde.

3. LAGVAL och DEFINITIONER

3.1 Vid Biträdets Behandling av Personuppgifter ska svenska lag och Tillämplig Dataskyddslagstiftning tillämpas. Biträdet ansvarar för att utföra all Behandling av Personuppgifter för Vårdgivarens räkning i enlighet med svensk lagstiftning och Tillämplig Dataskyddslagstiftning.

3.2 Med ”**Tillämplig Dataskyddslagstiftning**” ska förstås vad som anges under punkterna a. och b. nedan.

a. Rådsdirektiv 95/46/EG, införd i svensk rätt genom personuppgiftslagen (1998:204) och personuppgiftsförordningen (1998:1191) samt den allmänna dataskyddsförordningen (EU) 2016/679 (”**GDPR**”), med tillhörande genomförandeförfattningar. I händelse av motstridigheter mellan ovan nämnda författningar ska GDPR från och med den 25 maj 2018 ha företräde.

b. Datainspektionens, eller annan tillsynsmyndighets, bindande föreskrifter och beslut som är tillämpliga på Behandling av Personuppgifter inom ramen för detta Biträdesavtal.

3.3 Övriga begrepp med stor begynnelsebokstav i detta Biträdesavtal ska tolkas i enlighet med Tillämplig Dataskyddslagstiftning.

4. OMFATTNING

Biträdesavtalet avser Behandling av Personuppgifter enligt nedan.

4.1 Kategorier av Registrerade

De Personuppgifter som ska behandlas rör följande kategorier av Registrerade:

1. Patienter.
2. XX
3. XX

4.2 Typen av Personuppgifter som behandlas  
  
De Personuppgifter som behandlas är av följande slag:

1. Personnummer.
2. Namn.
3. Adress.
4. Telefonnummer.
5. Hälsotillstånd.
6. XX
7. XX

*Känsliga Personuppgifter (i förekommande fall)*

* 1. Personuppgifter om hälso - och sjukvård.
  2. XX

4.3 Behandlingens art

Personuppgifterna kommer att behandlas på följande sätt:

1. Organisering.
2. Lagring.
3. Bearbetning eller ändring.
4. Återvinning.
5. Inhämtande.
6. Användande.
7. Utlämnande genom översändande.
8. Sammanställning.
9. Behandlingar sker av känsliga uppgifter så som Personuppgifter som rör hälso- och sjukvård samt uppgifter som är sekretessbelagda.

4.4 Ändamålet med Behandlingen

Behandlingen av Personuppgifter sker i syfte att:

1. Kunna upprätta patientjournal samt föra dokumentation.
2. Bokning av patientbehandlingar.
3. XX
4. XX
5. XX
6. Ta ut aktuell statistik.

5. Behandling av Personuppgifter

5.1 Biträdet ska endast Behandla Personuppgifter i enlighet med detta Biträdesavtal, Huvudavtalet och dess bilagor, Tillämplig Dataskyddslagstiftning och Vårdgivarens, vid var tid, meddelade instruktioner. Biträdet får endast behandla Personuppgifter på dokumenterade instruktioner från Vårdgivaren.

5.2 Biträdet får inte behandla Personuppgifterna för något annat ändamål eller på något annat sätt än vad som är nödvändigt för att tjänsterna enligt Huvudavtalet ska kunna utföras.

5.3 Biträdet får inte

1. Samla in andra Personuppgifter än vad som avtalats mellan Vårdgivaren och Biträdet.
2. Ändra metod för Behandling.
3. Kopiera eller återskapa Personuppgifter eller på annat sätt behandla Personuppgifter för andra ändamål än de som anges i Huvudavtalet.

5.4 Biträdet ska utan dröjsmål vidta rättelse (rätta, radera, blocka, ändra eller gallra) Personuppgifter enligt Vårdgivarens instruktioner. Om Vårdgivaren skriftligen begärt rättelse av Personuppgift får Biträdet endast behandla Personuppgiften som ett led i rättelseprocessen och åtar sig att vidta åtgärden utan dröjsmål, dock senast inom 90 dagar.

6. Incidentrapportering

6.1 För det fall Biträdet misstänker alternativt upptäcker någon säkerhetsöverträdelse så som obehörig åtkomst, förstörelse, ändring eller liknande av Personuppgifter, eller om Biträdet av någon annan anledning inte kan uppfylla åtaganden i detta Biträdesavtal ska Biträdet omedelbart

1. undersöka incidenten och vidta lämpliga åtgärder för att läka incidenten och förhindra en upprepning och
2. tillhandahålla Vårdgivaren en beskrivning av incidenten.

6.2 Beskrivningen av incidenten ska åtminstone:

1. 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,
2. förmedla namnet på och kontaktuppgifterna för Biträdets dataskyddsombud eller andra kontaktpunkter där Vårdgivaren kan erhålla mer information,
3. beskriva de sannolika konsekvenserna av personuppgiftsincidenten och
4. beskriva de åtgärder som Biträdet har vidtagit eller föreslagit för att åtgärda Personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

6.3 Biträdet ska med beaktande av typen av Behandling samt den information som Biträdet har att tillgå bistå Vårdgivaren så att skyldigheten att informera den Registrerade vid en Personuppgiftsincident i enlighet med Tillämplig Dataskyddslagstiftning fullgörs.

7. Konsekvensbedömning avseende dataskydd och förhandssamråd

7.1 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 Biträdet före Behandlingen utförs vara Vårdgivaren 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.

7.2 För det fall bedömningen av den planerade Behandlingen visar att Behandlingen skulle leda till hög risk om Vårdgivaren inte vidtar åtgärder för att minska risken ska Biträdet före Behandlingen utförs vara Vårdgivaren behjälplig vid samråd med tillsynsmyndigheten.

8. Underleverantör

8.1 Biträdet har inte rätt att anlita underleverantör för utförande av Behandling av Personuppgifter för Vårdgivarens räkning, utan Vårdgivarens skriftliga godkännande.

8.2 Om Biträdet har för avsikt att anlita underleverantör enligt ovan, ska Biträdet tillse att sådan underleverantör genom undertecknande av avtal åtar sig samma skyldigheter som åligger Biträdet enligt Biträdesavtalet och att detta presenteras för Vårdgivaren för godkännande.

9. BEHANDLING AV PERSONUPPGIFTER I TREDJE LAND

9.1 Biträdet får inte utan Vårdgivarens skriftliga medgivande föra över Personuppgifter till tredje land, dvs till land utanför EU eller EES-området. Förbudet att överföra Personuppgifter enligt ovan omfattar även teknisk support, underhåll och liknande tjänster.

9.2 Har Biträdet erhållit Vårdgivarens skriftliga medgivande att föra över Personuppgifter till tredje land ska Biträdet ansvara för att säkerställa att överföring till tredje land sker med upprätthållande av adekvat skyddsnivå enligt svensk lag och Tillämplig Dataskyddslagstiftning.

10. Säkerhetsåtgärder

10.1 Biträdet ska bedriva sin verksamhet på sätt som säkerställer att bestämmelserna i   
Tillämplig Dataskyddslagstiftning om adekvat skydd för Behandlingar av Personuppgifter efterlevs. Biträdet ska, efter den 25 maj 2018, vidta alla åtgärder som krävs enligt artikel 32 i Dataskyddsförordningen.

10.2 Biträdet ska dokumentera rutiner och åtgärder för att uppfylla dessa säkerhetskrav. Dokumentationen ska hållas tillgänglig för Vårdgivaren. För det fall att Biträdet bedömer att det saknas instruktioner som är nödvändiga för att genomföra uppdraget enligt vad som sägs i detta Biträdesavtal ska Biträdet utan dröjsmål informera Vårdgivaren om sin inställning, ange om fullgörandet av Huvudavtalet kan påverkas av behovet av instruktioner samt invänta vidare instruktioner från Vårdgivaren.

10.3 Vidare ska Biträdet vidta lämpliga tekniska och organisatoriska åtgärder för att skydda Personuppgifterna från obehörig åtkomst, förstörelse eller ändring. De åtgärder   
Biträdet ska vidta, ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

1. de tekniska möjligheter som finns,
2. kostnaderna för att genomföra åtgärderna,
3. de särskilda risker som finns med den aktuella Behandlingen av Personuppgifter och
4. hur pass känsliga de Personuppgifter som behandlas är.

10.4 Biträdet ska därvid särskilt iaktta föreskrifter eller rekommendationer från tillsynsmyndigheter som har en styrande inverkan på Vårdgivarens verksamhet och som ger vägledning vad gäller informationssäkerhet.

10.5 De tekniska och organisatoriska säkerhetsåtgärder som Biträdet ska vidta ska minst omfatta följande.

* 1. Åtkomstskydd. När datorutrustning och löstagbara datamedier hos Biträdet inte står under uppsikt ska utrustningen och medierna låsas in för att skyddas mot obehörig användning, påverkan och stöld. I annat fall ska Personuppgifterna krypteras. För det fall eventuella bärbara datorer används vid Behandlingar ska Personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.
  2. Säkerhetskopia. Personuppgifterna ska regelbundet överföras till säkerhetskopior. Kopiorna ska förvaras avskilt och väl skyddade så att Personuppgifterna kan återskapas efter en störning. Biträdet ska ha en rutin för test av återläsning.
  3. Behörighetskontroll. Ett tekniskt system för behörighetskontroll ska styra åtkomsten till Personuppgifterna för Biträdet. Behörigheten ska begränsas till dem som behöver uppgifterna för sitt arbete. Användaridentitet och lösenord ska vara personliga och får inte överlåtas på någon annan. Det ska finnas rutiner för tilldelning och borttagande av behörigheter.
  4. Loggning. Åtkomst till Personuppgifter ska kunna följas upp i efterhand genom en logg eller liknande underlag. Underlaget ska kunna kontrolleras av Biträdet och återrapporteras till den Vårdgivaren.
  5. Datakommunikation. Anslutning för extern datakommunikation ska skyddas med sådan teknisk funktion som säkerställer att uppkopplingen är behörig. För åtkomst till Känsliga och Integritetskänsliga Personuppgifter krävs tvåfaktorsautentisering. Personuppgifter som överförs via datorkommunikation utanför lokaler som kontrolleras av Biträdet ska skyddas med kryptering.
  6. 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.
  7. Reparation och service. När reparation och service av datorutrustning, vilken används för att lagra Vårdgivarens Personuppgifter, utförs av annan än Biträdet, ska avtal som reglerar säkerhet och sekretess träffas med serviceföretaget. Vid servicebesök ska servicen ske under Biträdets överinseende. Är detta inte möjligt ska lagringsmedier som innehåller Personuppgifter avlägsnas. Service via fjärrstyrd datakommunikation får endast ske efter säker elektronisk identifiering av den som utför servicen. Servicepersonal ska ges åtkomst i systemet endast.

I Vårdgivarens instruktioner till Biträdet och/eller i Huvudavtalet, kan förekomma mer specifika krav på säkerhetsåtgärder.

10.6 Biträdet ska säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstankar om att användare hos såväl Vårdgivaren som Biträdet har haft obehörig åtkomst till informationen.

10.7 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 Biträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

1. pseudonymisering och kryptering av Personuppgifter,
2. förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemen och tjänsterna,
3. förmågan att återställa tillgängligheten och tillgången till Personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och
4. 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.

10.8 Biträdet ska Behandla Personuppgifter på utrustning som fysiskt befinner sig i Sverige.

11. granskning

11.1 Vårdgivaren har rätt att på egen bekostnad själv, eller med hjälp av Vårdgivaren utsedd representant, genomföra revision gentemot Biträdet och på annat sätt kontrollera att Biträdet uppfyller sina åtaganden enligt Biträdesavtalet och Tillämplig Dataskyddslagstiftning. Biträdet ska möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av Vårdgivaren utsedd representant. Biträdet ska lämna Vårdgivaren den assistans och tillhandahålla den dokumentation som erfordras för detta. Vårdgivaren, eller av Vårdgivaren utsedd representant, ska ha rätt till inspektion av den hårdvara och mjukvara som används för Behandling av Personuppgifter som omfattas av Biträdesavtalet samt tillträde till de fysiska lokaler där utrustning och annan hård- och mjukvara finns.

11.2 Om Vårdgivaren finner att Biträdet inte uppfyller kraven på lämplig säkerhetsnivå eller i annat avseende Behandlar Personuppgifter i strid med Biträdesavtalet är Biträdet skyldigt att omgående vidta rättelse efter Vårdgivarens påpekande. Om rättelse inte sker inom skälig tid efter Vårdgivarens skriftliga påpekande och avsaknaden av rättelse kan medföra olägenhet för Vårdgivaren har Vårdgivaren rätt att säga upp Biträdesavtalet och Huvudavtalet till omedelbar upphörande.

11.3 Biträdet ska på begäran från Vårdgivaren tillhandahålla all tillgänglig information avseende Behandlingen av Personuppgifter samt de resurser som krävs för att Vårdgivaren ska kunna säkerställa att Biträdet uppfyller sina skyldigheter enligt Biträdesavtalet och Tillämplig Dataskyddslagstiftning. Biträdet ska vidare ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i artikel 32 i Dataskyddsförordningen har fullgjorts samt i övrigt tillhandahålla all tillgänglig information samt nödvändiga resurser för att Vårdgivaren ska kunna följa sina skyldigheter enligt Tillämplig Dataskyddslagstiftning eller annat avtal.

11.4 Biträdet åtar sig att årligen revidera säkerheten i Behandlingen av Personuppgifter genom en intern revision för att kontrollera att Biträdets behandling av Personuppgifter följer detta Biträdesavtal. Resultatet ska delges Vårdgivaren.

11.5 Biträdet ska omedelbart informera Vårdgivaren om:

* 1. Biträdet får kännedom om att Personuppgifter behandlas i strid med Vårdgivarens instruktioner eller Tillämplig Dataskyddslagstiftning.
  2. Biträdet anser att en instruktion från Vårdgivaren strider mot Tillämplig Dataskyddslagstiftning.

12. utlämnande av information

12.1 Biträdet ska ha genomfört de lämpliga tekniska och organisatoriska åtgärder som krävs för att hjälpa Vårdgivaren så att Vårdgivaren kan fullgöra sin skyldighet att svara på begäran om utövande av den Registrerades rättigheter i enlighet med kapitel III i Dataskyddsförordningen. Biträdet ska bistå Vårdgivaren för det fall en Registrerad begär att få ta del av information som finns Registrerad om denne eller begär rättelse av sådan information  
  
För det fall att Registrerad, Datainspektionen eller annan tredje man begär information från Biträdet som rör Behandling av Personuppgifter ska Biträdet hänvisa till Vårdgivaren. Biträdet får inte lämna ut Personuppgifter eller annan information om Behandlingen av Personuppgifterna utan skriftligt medgivande från Vårdgivaren. Biträdet ska bistå Vårdgivaren för det fall den Registrerade begär att få ta del av information som finns Registrerad om denne i form av Personuppgifter eller begär rättelse av sådan information.

12.2   Biträdet ska utan dröjsmål skriftligen informera Vårdgivaren om eventuella kontakter från Datainspektionen eller annan tillsynsmyndighet som rör eller kan vara av betydelse för Behandling av Personuppgifter. Biträdet har inte rätt att företräda Vårdgivaren eller agera för Vårdgivarens räkning gentemot Datainspektionen eller andra tillsynsmyndigheter som rör eller kan vara av betydelse för Behandling av Personuppgifter. För det fall Biträdet genom lag eller myndighetsföreläggande är tvungen att lämna ut Personuppgifter, gäller vad som stadgas i punkt 13.3.

13. Sekretess

13.1 Biträdet och de personer som arbetar under dennes ledning ska vid Behandling av Personuppgifter iaktta sekretess. Det innebär att Personuppgifter eller annan information som Biträdet erhållit till följd av Behandling av Personuppgifter enligt Biträdesavtalet inte obehörigen får röjas för tredje man.

13.2 Biträdet ska inom sin organisation särskilt begränsa åtkomsten till Personuppgifter till personer som behöver sådan åtkomst för att fullgöra sina arbetsuppgifter. Biträdet ska se till att de personer som har åtkomst till Personuppgifterna följer Biträdets sekretesskyldighet enligt denna punkt 13 samt att de är informerade om hur de får Behandla Personuppgifterna.

13.3 Biträdet får lämna ut Personuppgifter utan att det innebär ett handlande i strid med Biträdesavtalet om Biträdet genom lag eller myndighetsföreläggande är tvungen att lämna ut Personuppgifter. I sådant fall åligger det Biträdet att omgående skriftligen meddela Vårdgivaren om detta och att begära att de efterfrågade Personuppgifterna omfattas av sekretess vid utlämnandet.

13.4 Sekretesskyldighet gäller även om Biträdesavtalet i övrigt upphör.

14. Ansvar gentemot tredje man

Biträdet ska hålla Vårdgivaren skadeslös för det fall Vårdgivaren drabbas av skada till följd av Biträdets Behandling av Personuppgifter i strid med Biträdesavtalet, Vårdgivarens instruktioner eller att Biträdet i övrigt agerat i strid med Tillämplig Dataskyddslagstiftning. Ersättningsskyldigheten gäller även om Biträdesavtalet i övrigt upphör.

15. Ersättning

Biträdet har inte rätt till särskild ersättning för Behandling av Personuppgifter och övriga åtaganden enligt Biträdesavtalet.

16. ändringar i Biträdesavtalet

16.1 Vårdgivaren får ändra innehållet i Biträdesavtalet i den mån så erfordras för att tillgodose krav som följer av Tillämplig Dataskyddslagstiftning eller annan registerförfattning som omfattar Vårdgivarens verksamhet. Ändring ska träda i kraft 30 dagar efter att skriftligt meddelande om ändring kommit Biträdet tillhanda.

16.2 Övriga ändringar av och tillägg till Biträdesavtalet ska för att vara bindande upprättas skriftligen och vara behörigen undertecknade av Parterna.

17. Avtalstid och Biträdesavtalets upphörande

17.1 Biträdesavtalet löper med start från den dag bägge Parter undertecknat Biträdesavtalet och gäller så länge som Biträdet behandlar Vårdgivarens Personuppgifter enligt Huvudavtalet.

17.2 Vid Biträdesavtalets upphörande ska Biträdet, beroende på vad Vårdgivaren beslutar, antingen (i) till Vårdgivaren överlämna alla Personuppgifter som behandlats enligt detta Biträdesavtalet eller (ii) förstöra alla Personuppgifterna. I samband med sådan åtgärd ska Biträdet skriftligen intyga för Vårdgivaren att alla Personuppgifter överlämnats eller, i förekommande fall, förstörts och att Biträdet inte längre har Personuppgifterna i behåll.

18. tvist

Tvist med anledning av detta Biträdesavtalet ska avgöras enligt bestämmelserna därom i Huvudavtalet Parterna emellan. I den mån det inte finns sådan reglering i Huvudavtalet ska tvisten avgöras av allmän domstol.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Biträdesavtalet har upprättats i två (2) originalexemplar, varvid Parterna undertecknat och tagit var sitt exemplar. Samtliga Biträdesavtalets sidor har undertecknats av Parterna med nedan angivna ställföreträdares initialer.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Ort |  | Ort |
| Datum |  | Datum |
| Vårdgivaren |  | Biträdet |
| Underskrift genom behörig företrädare |  | Underskrift genom behörig företrädare |
| Namnförtydligande |  | Namnförtydligande |