|  |
| --- |
|  |

Personuppgiftsbiträdesavtal

# Parter

## Personuppgiftsansvarig (”PuA”): Vårdgivare (org.nr.: xxxxxx-xxxx) med adress Box xxxx, xxx xx Stad.

## Personuppgiftsbiträde (”PuB”): Region Jönköpings län, Nämnden för folkhälsa- och sjukvård (org.nr: 232100-0057) med adress Box 1024, 551 11 Jönköping.

# Definitioner

## Med ”Personuppgifterna” avses sådana personuppgifter som enligt detta avtal behandlas av PuB för PuA:s räkning.

## Med ”Tillämplig dataskyddslag” avses i detta avtal vid var tid gällande lydelse av Dataskyddsförordningen[[1]](#footnote-1) samt annan eventuell EU- och nationell lagstiftning (inklusive förordningar och föreskrifter) som är tillämplig på behandling av personuppgifter enligt detta avtal.

## I den mån Tillämplig dataskyddslag innehåller begrepp som motsvarar de som används i detta avtal, ska sådana begrepp tolkas och tillämpas i enlighet med respektive regelverk.

# Bakgrund och syfte

## eFrikort är en av PuB, genom CGI Sverige AB, tillhandahållen e-tjänst för att vårdgivare ska kunna hantera patienters högkostnadsskydd och frikort. Tjänsten är en molntjänst och alla personuppgifter lagras hos CGI Sverige AB. PuA och PuB har 2019-XX-XX ingått Anslutningsavtalet. Detta Biträdesavtal är tillämpligt om och i den utsträckning den tjänst som PuB tillhandahåller innebär att PuB som personuppgiftsbiträde behandlar personuppgifter för PuA:s räkning. Detta Biträdesavtal utgör en bilaga till Anslutningsavtalet.

## Om det finns oförenliga eller motstridiga villkor beträffande behandling av personuppgifter, avseende den tjänst som beskrivs i detta avtal 3.1, i avtal eller annan överenskommelse mellan PuA och PuB, ska villkoren i detta avtal äga företräde. Detta avtal ersätter eventuella tidigare personuppgiftsbiträdesavtal mellan parterna.

## Detta avtal har till syfte att säkerställa de registrerades fri- och rättigheter vid behandling av personuppgifter samt att uppfylla kravet på skriftlig reglering av villkoren för anlitande av personuppgiftsbiträde enligt Dataskyddsförordningens artikel 28.3.

# Omfattning

## Föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade framgår av ifylld Mall för Instruktion och Avrop (bilaga 1).

# PuA:s ansvar

## PuA ansvarar för att det finns lagstöd för behandlingen av Personuppgifterna och att i övrigt följa Tillämplig dataskyddslag.

## PuA åtar sig att, i den mån så krävs utöver detta avtal och eventuell annan avtalsreglering parterna emellan, utforma ytterligare skriftliga instruktioner för behandlingen av Personuppgifterna som är förenliga med Tillämplig dataskyddslag och som behövs för att PuB ska kunna fullgöra sina uppgifter enligt avtalet.

## PuA åtar sig att utan dröjsmål informera PuB om förändringar i behandlingen vilka påverkar PuB:s skyldigheter enligt detta avtal och Tillämplig dataskyddslag.

# PuB:s allmänna åtaganden

## PuB åtar sig att endast behandla Personuppgifterna för att fullgöra sina uppgifter enligt detta avtal och endast på sätt som framgår av avtalet och/eller PuA:s skriftliga instruktioner.

## Kravet på skriftliga instruktioner gäller särskilt, men inte begränsat till, sådan behandling som består i utlämnande av Personuppgifterna till myndighet eller annan utomstående samt överföring av Personuppgifterna till tredje land (se avsnitt 11).

## PuB åtar sig att följa Tillämplig dataskyddslag och hålla sig informerad om gällande rätt på området.

## PuB åtar sig att följa Datainspektionens eller annan behörig tillsynsmyndighets fattade beslut om åtgärder för att uppfylla kraven enligt Tillämplig dataskyddslag.

## PuB ska omedelbart informera PuA om PuB anser att lämnade instruktioner strider mot lag eller är otydliga och därefter invänta ytterligare instruktioner eller förtydliganden från PuA. Detsamma gäller om PuB anser att det saknas tillräckliga instruktioner för att genomföra behandlingen.

## PuB ska förvalta tjänster i enlighet med anslutna vårdgivares instruktioner om styrning och kontroll samt att genom avtal säkerställa att även leverantören av e-frikort följer dessa instruktioner. Förvaltningen ska även omfatta bemanning och styrning av central förvaltning, underhåll och fortlöpande utveckling av systemet eller tjänsten samt fortlöpande anpassning av systemet så att nödvändiga regelverk kan hållas aktuella och utvecklade

## PuB ska agera som beställare gentemot leverantören av e-frikort, innefattande bl. a. ett åtagande att ta ett samordningsansvar för e-frikort på beställarnivå och samordna samarbete och kommunikation med å ena sidan leverantören, å andra sidan anslutna vårdgivare.

# Säkerhet och sekretess

## PuB ska vidta de lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Tillämplig dataskyddslag samt lämnade instruktioner för att skydda Personuppgifterna. Säkerhetsåtgärderna ska fastställas bland annat med beaktande av samtliga de omständigheter och möjliga åtgärder som anges i Dataskyddsförordningens art. 32.

## Eventuella särskilda krav på säkerhetsåtgärder framgår av ifylld Mall för Instruktion och Avrop (bilaga 1).

## Vidtagna säkerhetsåtgärder ska dokumenteras och dokumentationen ska på begäran tillhandahållas PuA.

## PuB åtar sig att endast ge åtkomst till Personuppgifterna för personer inom sin egen organisation eller hos eventuell underleverantör som behöver tillgång till dem för att kunna utföra sina arbetsuppgifter inom ramen för detta avtal.

## PuB och de personer som arbetar under ledning av PuB (inklusive ev. konsulter och underleverantörer) ska vid behandlingen av Personuppgifterna hålla Personuppgifterna konfidentiella och får inte röja dem för obehöriga annat än enligt skriftliga instruktioner från PuA. PuB ansvarar för att samtliga personer som kommer i kontakt med Personuppgifterna är bundna av sekretess/tystnadsplikt enligt lag och/eller personliga avtal.

## PuB ska bistå PuA med att se till att de skyldigheter som enligt Tillämplig dataskyddslag åligger PuA vad gäller t.ex. säkerhetsåtgärder, konsekvensbedömningar, incidentrapportering och samråd kan fullgöras samt samråda kring lämpliga rutiner för detta.

## Skulle nya omständigheter som kan påverka informationssäkerheten uppkomma under avtalets giltighetstid ska PuB meddela PuA detta omgående så att parterna tillsammans kan vidta säkerhetshöjande åtgärder.

# De registrerades rättigheter

## PuB åtar sig att bistå PuA genom lämpliga tekniska och organisatoriska åtgärder vad gäller begäran från registrerade om att utöva deras rättigheter enligt Tillämplig dataskyddslag, exempelvis rättelse, radering eller begränsning av behandling, i den mån dessa rättigheter är tillämpliga på Personuppgifterna.

## För det fall en registrerad eller annan tredje part begär ut information från PuB rörande behandlingen av Personuppgifterna, eller om PuB tar emot en begäran om rättelse, radering, begränsning av behandling eller överföring, ska PuB hänvisa till PuA. PuB ska inte vidta någon åtgärd eller lämna ut någon information till registrerade eller annan tredje part om inte utlämnande krävs enligt tvingande lag. I så fall ska PuB omedelbart informera PuA om begäran.

# Revision, insyn och tillsyn

## För att kunna säkerställa att PuB vidtar tillräckliga säkerhetsåtgärder och även i övrigt fullgör sina skyldigheter enligt detta avtal, har PuA rätt till nödvändig insyn i PuB:s verksamhet. PuB åtar sig att på PuA:s begäran utan dröjsmål tillhandahålla den information som PuA behöver för att kunna utöva insyn.

## PuB ska tillåta och möjliggöra de inspektioner som Datainspektionen eller PuA kan kräva för att kontrollera upprätthållandet av en korrekt och säker behandling av Personuppgifterna. Detta inbegriper att möjliggöra och bidra till granskningar samt inspektioner hos PuB eller ev. underleverantörer.

# Personuppgiftsincidenter

## En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till Personuppgifterna (se Dataskyddsförordningen art. 4).

## Om PuB får kännedom om en personuppgiftsincident med avseende på Personuppgifterna, ska denne utan onödigt dröjsmål informera PuA. PuB ska därvid bistå PuA i framtagandet av information och incidentrapporter till registrerade personer och till myndigheter i den utsträckning det krävs enligt Tillämplig dataskyddslag. PuB ska utan dröjsmål undersöka incidenten och i samråd med PuA vidta lämpliga åtgärder för att förhindra en upprepning.

## PuB ska omgående informera PuA även om åtaganden enligt detta avtal av någon annan anledning än en personuppgiftsincident inte uppfylls eller inte kommer att kunna uppfyllas.

# Överföring av personuppgifter till tredje land

## Överföring av Personuppgifterna till tredje land, dvs. ett land utanför EU/EES, eller en internationell organisation får endast ske om landet eller organisationen genom beslut enligt Dataskyddsförordningens artikel 45 har bedömts säkerställa en adekvat skyddsnivå för personuppgifter eller efter skriftligt godkännande av PuA i det enskilda fallet efter att PuA gjord bedömningen att överföringen är lämplig och tillåten på grund av vidtagna skyddsåtgärder enligt Dataskyddsförordningens artikel 46.

## Villkoren i detta avsnitt för överföring av Personuppgifterna ska gälla såväl överföring för lagring och annan behandling som åtkomst till Personuppgifterna för exempelvis service, support, underhåll, utveckling eller liknande ändamål från tredje land eller en internationell organisation.

## PuB ska alltid samråda med PuA innan överföring till tredje land sker.

# Anlitande av annat personuppgiftsbiträde

## PuB får inte anlita ett annat personuppgiftsbiträde för behandling av Personuppgifterna utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av PuA. Om ett allmänt skriftligt tillstånd har erhållits, ska PuB informera PuA om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att PuA har möjlighet att göra invändningar mot sådana förändringar.

## Om PuB anlitar annat personuppgiftsbiträde enligt föregående punkt, så ansvarar PuB för att det andra personuppgiftsbiträdet innan behandlingen påbörjas genom ett skriftligt avtal åläggs samma skyldigheter beträffande behandlingen av Personuppgifterna som PuB har enligt detta avtal. Avtalet med det andra personuppgiftsbiträdet ska i relevanta delar på begäran kunna uppvisas för PuA.

## Om PuB anlitar annat personuppgiftsbiträde enligt föregående punkt, ansvarar PuB för att det andra personuppgiftsbiträdet fullgör alla åtaganden och iakttar alla begränsningar som anges i denna bilaga.

## PuB ska vid var tid föra en korrekt och uppdaterad lista över personuppgiftsbiträden som anlitats enligt detta avsnitt och på begäran uppvisa denna för PuA. Vid avtalstecknandet anlitade underleverantörer framgår av Förteckning över underbiträden (bilaga 2).

# Giltighetstid

## Detta biträdesavtal är giltigt så länge som PuB:s behandling av Personuppgifter på uppdrag av PuA pågår. Parterna kan dock överenskomma att detta avtal ska ersättas av ett annat biträdesavtal.

## Åtagandena rörande sekretess och tystnadsplikt ska äga giltighet även efter detta avtal i övrigt har upphört att gälla.

# Upphörande av behandling av personuppgifter

## Vid upphörande av PuB:s uppdrag ska Personuppgifterna, på samtliga media som de är lagrade på, återlämnas till PuA eller i enlighet med PuA:s instruktioner raderas eller överföras till annat personuppgiftsbiträde.

## För det fall PuB på grund av lag, förordning, föreskrift eller myndighetsbeslut är skyldigt att fortsätta att behandla Personuppgifterna, får Personuppgifterna endast behandlas i den mån det är absolut nödvändigt för att fullgöra denna skyldighet. PuB ska informera PuA om varför fortsatt behandling är nödvändig.

# Ersättning

## Om inte annat särskilt överenskommits har PuB inte rätt till ersättning för fullgörande av sina skyldigheter i detta avtal.

## PuB tillhandahåller e-frikortstjänsten och finansierar denna samt ombesörjer utskick till patienter. PuA svarar själv för alla sina kostnader för att integrera övriga vårdsystem med e-frikort samt att införa och använda e-frikortstjänsterna i verksamheten.

# Skadeslöshet

## Sanktionsavgifter enligt Dataskyddsförordningens artikel 83 ska alltid slutligen bäras av den part som påförts en sådan avgift.

# Ändringar och tillägg

## Ändringar av och tillägg till detta avtal ska vara skriftliga och undertecknade av behörig företrädare för båda parter.

# Tvist

## Tvist angående tolkning eller tillämpning av detta avtal ska, om annat inte skriftligen överenskommits, avgöras enligt svensk lag och av svensk allmän domstol med Jönköpings tingsrätt som första instans.

Detta avtal har upprättats i två likalydande exemplar, varav parterna tagit var sitt.

**Behörig företrädare för PuA** **Behörig företrädare för PuB**

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

Ort och datum Ort och datum

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

Underskrift Underskrift

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

Namnförtydligande Namnförtydligande

**Bilaga 1**  
Utöver vad som redan framgår av detta personuppgiftsbiträdesavtal ska PuB följa nedanstående instruktioner. I den mån så krävs kan i mallen hänvisas till ytterligare bilagor (t.ex. tjänsteavtal eller -specifikation, systembeskrivning m.m.).

|  |  |
| --- | --- |
| **Ändamål**  Specificera samtliga ändamål för vilka personuppgifter kommer behandlas av PuB. | Ändamålet med behandlingen är att kunna tillhandahålla en elektronisk frikortstjänst för att underlätta för kassapersonal och patient vid besök inom vården.   PuB ska även kontinuerligt utveckla och förbättra tjänsten och för att uppfylla detta uppdrag kan PuB behöva behandla personuppgifter. |
| **Kategorier av personuppgifter**  Specificera samtliga kategorier av personuppgifter som kommer behandlas av PuB. | Uppgifter som krävs för att beräkna en patients frikort, så som personnummer, HSA-Id för den enhet där vårdbesöket ägt rum och betald avgift för vårdbesöket samt namn och adress till patienter som uppnått frikort och skall erhålla ett fysiskt frikort med posten.  Särskilda kategorier av personuppgifter: Uppgift om hälsa  Extra skyddsvärda kategorier av personuppgifter: Personnummer HSA-id för vårdenhet där patient gjort vårdbesök anses som känslig uppgift. |
| **Kategorier av registrerade**  Specificera samtliga kategorier av registrerade vars uppgifter kommer behandlas av PuB. | Vårdpersonal  Patienter |
| **Överföring av personuppgifter**  Den omfattning som personuppgifter kan komma att överföras utanför EES i syfte att fullgöra uppdraget. | Nej |
| **Lagringsregler** | Alla personuppgifter lagras hos CGI Sverige AB. Lagringsreglerna följer av den instruktion som finns som bilaga till personuppgiftsbiträdesavtalet mellan PuB och CGI Sverige AB enligt nedan.  Åtgärder för att tillse att personuppgifter gallras under och efter avtalstiden när användningen inte längre är nödvändig för det ursprungliga ändamålet:  Under avtalstiden: Enligt Patientdatalagen skall alla loggar lagras i minst 5 år. Så snart som möjligt och senast inom 2 månader efter att 5 år passerats skall loggarna raderas.  Frikortsdata för respektive patient skall lagras i 24 månader för att kunna hantera aktuell frikortsperiod samt se historik över frikort.  Ostrukturerat data i servicedesken/funktionsbrevlåda skall raderas inom 1 månad från att ärendet inkommit.  Filer för distribuering av fysiska frikort får lagras i maximalt 2 månader. |
| **Säkerhetsåtgärder**  Specificera kravställda/överenskomna säkerhetsåtgärder. | Alla personuppgifter lagras hos CGI Sverige AB. Säkerhetsåtgärderföljer av den instruktion som finns som bilaga till personuppgiftsbiträdesavtalet mellan PuB och CGI Sverige AB.  Instruktionen återfinns i detta avtal som Bilaga A. |

**Bilaga 2  
  
Förteckning över underbiträden**   
Uppge företagsnamn, syfte med behandling och land där personuppgiftsbiträden till PuB kommer att behandla PuA:s uppgifter.

|  |  |  |
| --- | --- | --- |
| **Namn** | **Syfte** | **Land** |
| **CGI Sverige AB** | **Leverantör av tjänsten enligt avtal, RJL 2018/2044** | **Sverige, Stockholm** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Bilaga 3  
  
Sammanställning av kontaktuppgifter   
  
Kontaktuppgifter personuppgiftsansvarig**  
**Dataskyddsombud**Namn:   
Telefonnummer:   
E-postadress:

**Kontaktperson**Namn:   
Telefonnummer:   
E-postadress:

**Kontaktuppgifter personuppgiftsbiträde**  
**Dataskyddsombud**Namn: Johan Cederlund  
Telefonnummer: 0702501226  
E-postadress: [dataskyddsombud@rjl.se](mailto:dataskyddsombud@rjl.se)

**Kontaktperson**Namn:  
Telefonnummer:  
E-postadress:

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 [↑](#footnote-ref-1)