

Personuppgiftsbiträdesavtal

1. PARTER

Detta personuppgiftsbiträdesavtal (Biträdesavtal) har dagen för undertecknande ingåtts mellan parterna:

PERSONUPPGIFTSANSVARIG (PUA)

Namn och adress:

Region Örebro län
Box 1613
701 16 Örebro

Organisationsnummer:

232100-0164

PERSONUPPGIFTSBITRÄDET (PUB)

Namn och adress:

Institutet för kvalitetsindikatorer i Fenix AB
Box 9129
400 93 Göteborg

Organisationsnummer:

556882-3404

Namn på en tjänst eller ett system som avses i detta Biträdesavtal

Detta personuppgiftsbiträdesavtal är en del av ett huvudavtal om tillhandahållandet av tjänster som ingåtts mellan Sveriges Kommuner och Landsting och leverantören för Hälso- och sjukvårdsbarometern 2023-2026 (Referensnummer 22/87).

Var för sig benämnda "Part" och tillsammans "Parterna".

2. DEFINITIONER

2.1 Nedanstående begrepp ska ha följande innebörd:

- a. *Tillämplig lag*, avser Europaparlamentets och rådets förordning (EU) 2016/679 (Dataskyddsförordningen), med tillhörande genomförandeförfattningar samt Datainspektionens, eller relevant EU-organs, föreskrifter, ställningstaganden och rekommendationer på dataskyddsområdet.
- b. *Underbiträde*, avser sådan underleverantör som anlitas av det personuppgiftsbiträde som är Part i detta Biträdesavtal och som behandlar personuppgifter för personuppgiftsansvariges räkning.
- c. *Standardavtalsvillkor*, avser Kommissionens beslut av den 5 februari 2010 (2010/87/EU), om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG eller motsvarande villkor som ersätter dessa.
- d. *Tredje land*, avser ett land som inte är medlem i Europeiska unionen (EU) eller Europeiska ekonomiska samarbetsområdet (EES- Island, Liechtenstein och Norge) samt ett land som av Europeiska Kommissionen inte anses uppfylla en adekvat skyddsnivå i förhållande till Tillämplig lag.
- e. *Tjänsteavtalet*, det avtal som har upprättats mellan PUA och PUB angående tillhandahållande av en tjänst eller inköp av ett system.

Ange namn på tjänsteavtalet och datum för undertecknande:

Hälso- och sjukvårdsbarometern (Referensnummer 22/87) som ingåtts mellan Sveriges Kommuner och Landsting och Institutet för kvalitetsindikatorer Fenix AB 2023-01-17

2.2 Alla begrepp i detta Biträdesavtal ska ha den betydelse som motsvarande begrepp i artikel 4 i Dataskyddsförordningen.

3. INNEHÅLL OCH SYFTE

- 3.1 Enligt Tillämplig lag ska all behandling av personuppgifter utförd av ett PUB för PUA:s räkning regleras genom avtal. Parterna är därmed överens att behandling av personuppgifter ska regleras enligt nedan.
- 3.2 De personuppgifter (Personuppgifter) som PUB får behandla på uppdrag av PUA ska anges i *bilaga 1* i detta Biträdesavtal.
- 3.3 I de fall det aktualiseras är PUB informerat om att PUA i situationer agerar som PUB för kunders räkning. Vid hantering av Personuppgifter kan PUB i förkommande fall därmed komma att agera som underbiträde. I roll som underbiträde har PUB identiska skyldigheter vid hantering av Personuppgifter enligt detta Biträdesavtal. Villkoren i detta Biträdesavtal är gällande även för det fall att PUB agerar som underbiträde.
 - 3.3.1 På PUB:s begäran kan en fullständig lista på de aktuella PUA biläggas till detta Biträdesavtal.

4. ANSVAR OCH INSTRUKTION

4.1 Personuppgiftsansvariges ansvar

- 4.1.1 PUA har ansvar för all behandling av avtalade Personuppgifter i enlighet med Tillämplig lag.
- 4.1.2 PUA får endast tillhandahålla PUB sådana personuppgifter som är nödvändiga för det bestämda ändamålet med behandlingen samt säkerställa att det finns en laglig grund för aktuella behandlingar av Personuppgifter.
- 4.1.3 PUA ska utforma och tillhandahålla PUB dokumenterade instruktioner, *bilaga 1*, och övriga anvisningar avseende ändamålet, omfattningen, arten och varaktigheten av behandlingen samt kategorier av registrerade i den utsträckning som är nödvändig för att PUB ska kunna uppfylla sina skyldigheter enligt detta Biträdesavtal och Tillämplig lag.

4.2 Personuppgiftsbitrådets ansvar och behandling av Personuppgifter

- 4.2.1 PUB intygar att denne besitter nödvändig teknisk och organisatorisk kapacitet och förmåga, inbegripet tekniska lösningar, kompetens, ekonomiska och personella resurser, rutiner och metoder, att fullgöra sina skyldigheter enligt detta Biträdesavtal och att Tillämplig lag efterlevs.
- 4.2.2 PUB åtar sig att enbart behandla avtalade personuppgifter i enlighet med Tjänsteavtalet, detta Biträdesavtal och i enlighet med Tillämplig lag.
- 4.2.3 PUB får endast behandla personuppgifter i enlighet med PUA:s dokumenterade instruktioner, bilaga 1, såvida inte PUB är skyldig enligt författning att behandla personuppgifter för annat ändamål eller på annat sätt.
- 4.2.4 Har PUA lämnat ofullständiga eller felaktiga instruktioner ska PUB utan dröjsmål påtala detta för PUA och därefter invänta PUA:s anvisningar.
- 4.2.5 PUB ska upprätthålla ett register över all personuppgiftsbehandling som sker på uppdrag av PUA, samt att på PUA:s eller behörig tillsynsmyndighets uttryckliga begäran överlämna ett läsbart registerutdrag enligt artikel 30 punkt 2.
- 4.2.6 Om en typ av behandling som PUB ska utföra med anledning av detta Biträdesavtal, 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 PUB före behandlingen utföra vara PUA 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.



5. REVISION OCH SAMVERKAN

- 5.1 PUB åtar sig att minst en gång om året revidera säkerheten i personuppgiftsbehandlingen genom en intern revision för att kontrollera att PUB:s behandling av personuppgifter följer detta biträdesavtal. Resultatet ska på begäran delges PUA.
- 5.2 PUB ska åtminstone vart tredje år revidera säkerheten i personuppgiftsbehandlingen, genom en extern granskning av oberoende part, för att kontrollera att PUB:s behandling av personuppgifter följer detta biträdesavtal. Granskningsrapport ska delges PUA.
- 5.3 PUB ska, utan dröjsmål, på begäran av PUA tillhandahålla all tillgänglig information avseende behandlingen av personuppgifter genom att tillhandahålla relevant dokumentation, hänvisa till relevant och godkänd uppförandekod eller certifiering, möjliggöra och bidra till granskningar och inspektioner och/eller tillhandahålla PUA annan adekvat bevisning för att PUA ska kunna uppfylla sina skyldigheter som PUA enligt Tillämplig lag.
- 5.4 PUA äger rätt att, genom tredje man, som inte utgör en konkurrent till PUB, genomföra revision gentemot PUB eller på annat sätt kontrollera att PUB:s behandling av personuppgifter följer detta Biträdesavtal och som är nödvändiga för att PUA ska utöva en effektiv kontroll av de åtgärder som PUB utför. Vid sådan revision eller kontroll ska PUB bistå den som utför granskningen med dokumentation och andra tillgångar som behövs för att följa upp efterlevnad av detta Biträdesavtal.
- 5.5 PUB äger dock rätt att erbjuda alternativa tillvägagångssätt för uppföljning, exempelvis granskning genomförd av oberoende tredje part. PUA ska i sådant fall äga rätt, men inte vara skyldig att, tillämpa detta alternativa tillvägagångssätt för uppföljning. Vid sådan revision eller kontroll ska PUB ge PUA eller en tredje part den assistans som behövs för genomförandet.
- 5.6 För de fallen registrerade personer, behörig tillsynsmyndighet eller annan tredje man begär information från PUB rörande behandlingen av personuppgifter ska parterna samverka och utbyta information i nödvändig utsträckning. PUB får inte lämna ut personuppgifter eller information om behandlingen av personuppgifter utan skriftligt medgivande i förväg från PUA utom för det fall föreläggande finns därom från behörig tillsynsmyndighet eller om PUB är nödgad därtill enligt tvingande lagstiftning.
- 5.7 PUB ska vara PUA behjälplig genom lämpliga tekniska och organisatoriska åtgärder, så att PUA kan fullgöra sin skyldighet avseende de registrerades rättigheter.

6. ANLITANDE AV UNDERBITRÄDEN

- 6.1 PUB har rätt att anlita Underbiträde för fullgörandet av PUB:s åtaganden enligt Biträdesavtalet, förutsatt att:
- 6.1.1 PUB informerar PUA om sina avsikter att använda eller byta ut Underbiträde varpå PUA har rätt att göra invändningar mot en sådan förändring, samt
- 6.1.2 Underbiträdet genom ett så kallat underbiträdesavtal med PUB åläggs samma skyldigheter i fråga om dataskydd som de som fastställs i detta Biträdesavtal och framför allt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i Tillämplig dataskyddslag.
- För det fall, att PUB anlitar ett underbiträde i tredje land, ska PUB 1) ingå ett tilläggsavtal baserat på standardavtalsvillkor med underbiträdet i tredje land eller 2) säkerställa att adekvat skyddsnivå upprätthålls i enlighet med EU kommissionens beslut.

PUB:s information till PUA enligt denna punkt 6.1 ska innehålla uppgift om Underbiträdets namn, platsen för Behandlingen samt, på PUA:s skriftliga begäran, vilken typ av Behandling Underbiträdet ska utföra för PUB:s räkning. En kopia på ingånget underbiträdesavtal och eventuella standardavtalsvillkor ska utan onödigt dröjsmål på PUA:s begäran, skickas till PUA.

- 6.2 För det fall att PUA har invänt mot Underbiträde enligt punkt 6.1 ovan ska Parterna tillsammans diskutera möjliga åtgärder för att lösa orsaken till PUA:s invändning. Om Parterna inte kan komma överens om någon lösning inom en rimlig tid, har PUA rätt att omedelbart säga upp Tjänsteavtalet med PUB genom att meddela detta skriftligen till PUB.
- 6.3 PUA har rätt att återkalla ett godkännande av Underbiträdet om PUA bedömer att Underbiträdet inte efterlever skyldigheterna enligt Biträdesavtalet eller Tillämplig dataskyddslag.
- 6.4 PUB ska säkerställa att PUA har kännedom om vilka Underbiträden som Behandlar personuppgifter genom att, på begäran av PUA tillhandahålla PUA fullständig, korrekt och uppdaterad information om samtliga Underbiträden, där följande information specificeras för varje enskilt Underbiträde:
 - 6.4.1 definition av Underbiträdet, inklusive dess kontaktinformation, bolagsform och geografisk placering,
 - 6.4.2 vilken typ av tjänst som Underbiträdet utför,
 - 6.4.3 garantier som uppställs för att kraven i Tillämplig dataskyddslag kommer att följas, samt
 - 6.4.4 var Underbiträdet Behandlar personuppgifter som omfattas av Biträdesavtalet.
- 6.5 En lista på de Underbiträden som anlitas för behandling av personuppgifter framgår av Bilaga 2 till Biträdesavtalet.
- 6.6 Om Underbiträdet inte uppfyller sina skyldigheter i fråga om Behandling av personuppgifter enligt underbiträdesavtalet ska PUB förbli fullt ansvarig gentemot PUA för Underbiträdets uppfyllande av Underbiträdets skyldigheter enligt Biträdesavtalet samt Tillämplig dataskyddslag.

7. SÄKERHET OCH SEKRETESS

- 7.1 Avtalade åtgärder ska åstadkomma en säkerhetsnivå som PUA efter samråd med dataskyddsombudet bedömer lämplig, dock utan att inskränka de krav på säkerhetsåtgärder som föreskrivs i Tillämplig lag.
- 7.2 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 PUB vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt
 - a. pseudonymisering och kryptering av personuppgifter
 - b. förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna
 - c. förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk personuppgiftsincident
 - d. ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet

- 7.3 PUB ska ha ett behörighetskontrollsystem som förhindrar obehörig behandling av eller obehörig åtkomst till Personuppgifter. PUB ska använda ett loggsystem som möjliggör att behandling av Personuppgifter spåras samt tillse en adekvat skyddsnivå för dessa loggar.
- 7.4 För det fall PUB har fått vetskap om en personuppgiftsincident dvs. obehörig åtkomst, obehörigt röjande, förstörelse, ändring eller förlust av Personuppgifter ska PUB utan onödigt dröjsmål undersöka personuppgiftsincidenten och vidta lämpliga åtgärder för att hantera personuppgiftsincidenten och förhindra en upprepning. PUB ska omedelbart, skriftligen tillhandahålla PUA en beskrivning av personuppgiftsincidenten.
- 7.4.1 Beskrivningen av personuppgiftsincidenten ska åtminstone:
- a. 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,
 - b. förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
 - c. beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
 - d. beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.
- 7.5 PUB och den personal som arbetar under detta Biträdesavtal ska vid behandling av Personuppgifter iakttä sekretess, såväl handlingssekretess som tystnadsplikt.
- 7.6 PUB åtar sig att tillse att samtliga anställda, konsulter och övriga som PUB svarar för och som behandlar Personuppgifterna är bundna av en sekretessförbindelse.
- 7.6.1 Sekretessförbindelser krävs inte om PUB och dess personal omfattas av en straffsanktionerad tystnadsplikt som följer av lag.
- 7.7 I de fall PUB anlitar ett Underbiträde åtar sig PUB att tillse att det finns lämpliga sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och dess personal.
- 7.8 All information som PUB erhåller genom informationsutbyte enligt detta Biträdesavtal eller annat avtal mellan Parterna får inte utnyttjas eller röjas för annat ändamål än som framgår av detta Biträdesavtal eller annat avtal Parterna emellan, vare sig direkt eller indirekt, om inte PUA på förhand skriftligen medgivit detta.
- 7.9 PUB ska utan dröjsmål skriftligen underrätta PUA om eventuella kontakter med tillsynsmyndighet som rör eller kan vara av betydelse för behandling av Personuppgifter. PUB har inte rätt att företräda PUA eller agera för PUA:s räkning gentemot tillsynsmyndigheter i frågor som rör eller kan vara av betydelse för behandling av Personuppgifter.

8. ANSVAR FÖR SKADA

- 8.1 Vid ersättning för skada som, genom fastställd dom eller annat beslut, utgått till registrerad på grund av överträdelse av någon bestämmelse i detta avtal, instruktion från PUA eller tillämplig dataskyddsbestämmelse ska artikel 82 Dataskyddsförordningen tillämpas.
- 8.2 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen eller 6 kap. 2 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den Part som påförts en sådan avgift.
- 8.3 Om PUA får kännedom om omständighet som kan leda till skadestånd eller betalningsansvar för PUB ska PUA omedelbart informera PUB om förhållande och aktivt arbeta tillsammans med PUB för att förhindra och minimera sådant skadestånd eller betalningsansvar.
- 8.4 Oaktat vad som anges i Huvudavtalet och dess Bilagor gäller 8.1 och 8.2 före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser behandling av personuppgifter.

9. GILTIGHET, ÄNDRING OCH UPPHÖRANDE AV BEHANDLING AV PERSONUPPGIFTER

- 9.1 Detta Biträdesavtal gäller från dess undertecknande och så länge som PUB behandlar Personuppgifter för PUA:s räkning i enlighet med Tjänsteavtalet, eller om detta Biträdesavtal ersätts av ett annat personuppgiftsbiträdesavtal.
- 9.2 Tillägg och ändringar av detta Biträdesavtal ska, för att vara giltiga, vara skriftliga och undertecknas av båda Parter. En begäran om ändring av endera parten innebär inte att detta Biträdesavtal bryts utan endast att en omförhandling påbörjas.
- 9.3 PUB ska vid avslutad behandling och beroende på vad PUA väljer, radera eller återlämna de behandlande Personuppgifterna i ett allmänt och läsbart format till PUA inom skälig tid, dock senast inom trettio (30) dagar, efter att Tjänsteavtalet eller detta Biträdesavtal har upphört att gälla (beroende på vilket som inträffar först) och därefter radera Personuppgifter från alla system som använts vid behandlingen inbegripet alla kopior. Detta gäller även annan tillhörande information såsom, instruktioner, systemlösningar, beskrivningar eller andra handlingar som PUB erhållit genom informationsutbyte enligt detta Biträdesavtal.

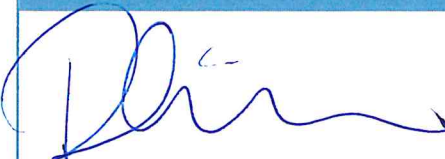
Detta gäller inte om åtgärden skulle strida med en annan tvingande lag.
- 9.4 Bestämmelser om sekretess i punkter 7.5-7.8 och bestämmelsen om upphörande av behandling i punkten 9.3 ska fortsätta gälla även efter upphörandet av detta Biträdesavtal.

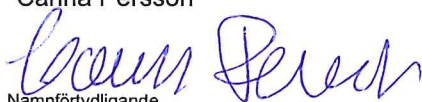
10. TVIST OCH TILLÄMPLIG LAG

- 10.1 Detta Biträdesavtal ska tolkas och tillämpas i enlighet med svensk rätt.
- 10.2 Alla tvister angående tolkning eller tillämpning av detta Biträdesavtal ska avgöras enligt Tjänsteavtalets bestämmelse om tvist. Vid avsaknad av en sådan bestämmelse ska tvister lösas i allmän domstol där PUA har sin hemvist.



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

Personuppgiftsansvarig Region Örebro län	Personuppgiftsbiträdet
	
Underskrift av ansvarig firmatecknare	Underskrift av ansvarig firmatecknare
Rickard Simonsson	
Namnförtydligande	Namnförtydligande
Örebro 21/4-23	
Ort och datum	Ort och datum

Kontaktperson PUA	Kontaktperson PUB
Carina Persson	
	
Namnförtydligande	Namnförtydligande
072-742 74 82	
Tfn	Tfn
carina.persson@regionorebrolan.se	
E-post	E-post

Bilaga 1 – Instruktion om hantering av personuppgifter

Utöver vad som redan framgår av detta avtal ska PUB även följa nedanstående instruktioner:

Personuppgiftsbehandling	
Ändamål (1) <i>Specificera samtliga ändamål för vilka personuppgifter som kommer behandlas av PUB är.</i>	Hälso- och sjukvårdsbarometern är en nationellt gemensam, årligt återkommande, undersökning av invånarnas förväntan på, uppfattning om och förtroende för svensk hälso- och sjukvård. Samtliga regioner deltar i undersökningen, som samordnas av SKR. Målet är att få underlag för uppföljning och förbättringsarbete i svensk hälso- och sjukvård, lokalt och nationellt.
Kategorier av personuppgifter (2) <i>Specificera kategorier av personuppgifter som kommer behandlas av PUB.</i>	Personuppgifter i systemet utgörs av följande uppgifter från SPAR eller motsvarande (befolkningsregister) • Namn • Adress • Ålder • Kön • Telefon-/mobilnummer • Geografisk tillhörighet
Känsliga personuppgifter (3) <i>Ange vilka särskilda kategorier av personuppgifter som behandlas</i>	Personuppgifter i systemet utgörs av följande uppgifter från enkätsvar • Ålder • Födelseland • Utbildningsnivå • Självskattad hälsa • Hälsa
Kategorier av registrerade (4) <i>Specificera samtliga kategorier av registrerade vars uppgifter kommer behandlas av PUB.</i>	Folkbokförda i Sverige, 18 år och äldre
Överföring av personuppgifter (5) <i>Den omfattning som personuppgifter kan komma att överföras utanför EES i syfte att tillhandahålla tjänsterna enligt Tjänsteavtalet.</i>	Personuppgiftsbiträdet ska tillse att personuppgifterna (hanteras och) lagras inom EU/EES. Personuppgiftsbiträdet äger ej rätt att överföra personuppgifter till tredje land.

Arkivering och gallring (6) <i>Specificera gallringstid avseende när personuppgifterna som behandlas av PUB ska gallras.</i>	Personuppgifter insamlade från SPAR eller motsvarande, ska gallras efter 6 månader. Säkerhetskopior får inte sparas längre än 1 år. Biträdet får ej självständigt publicera informationen eller vidarebefordra information för annans publicering.
Återlämning av data (7) <i>Ange hur PUB ska lämna tillbaka data efter avslutande behandling av Personuppgifter</i>	Personuppgifter hämtas ej från Region Örebro län. Endast avidentifierade enkätsvar levereras till Region Örebro län.
Informationssäkerhet och IT-säkerhet (8) <i>Ange de specifika krav som framkommit vid genomförande av informationsklassning och riskanalys utöver de krav som listas under Praktisk hantering på sidan 10-11 i detta Biträdesavtal.</i>	Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i Beställarens tjänst. Testdata ska skyddas och kontrolleras. Testdata ska ej inkludera information som är känslig eller omfattas av sekretess. Leverantören ska för de delar av verksamheten som berörs ha ett ledningssystem för informationssäkerhet (LIS) som baseras på ISO/IEC 27001 eller motsvarande. LIS ska omfatta bland annat att samtliga säkerhetskritiska administrativa och tekniska processer är dokumenterade och vilar på en formell grund där roller, ansvar och befogenheter finns tydligt definierade. Datahallen uppfyller minst skyddsnivå 3.
Särskilda instruktioner om behandlingen (9)	Leverantören ska skydda loggningsfunktioner och loggningsverktyg mot manipulation och obehörig åtkomst. Detta ska även omfatta leverantörens personal. Leverantören ska i sitt behörighetssystem logga information om när användare skapades, togs bort eller förändrades samt inloggningar. Loggningsfunktioner ska finnas för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning, överträdelser mot behörigheter. Leverantören ska ha dokumenterade rutiner för övervakning, upptäckt, analys, rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter. Leverantören ska ha avtal om tystnadsplikt med sina anställda.

1) Här ska framgå för vilka ändamål som personuppgifter kommer att behandlas: t.ex. PUB kommer att behandla personuppgifter för ändamålet att tillhandahålla tjänsten i enlighet med Avtalet, dvs support. Praktiskt rör det sig om att PUB kan behöva se patientinformation för att lösa användarproblem.

2) Här ska framgå vilka kategorier av personuppgifter som kommer att behandlas. t.ex. De personuppgifter som kommer att behandlas kan inkludera personuppgifter tillhörande följande kategorier:

- Personuppgifter hänförliga till den Personuppgiftsansvariges personal, i huvudsak kontaktuppgifter;
- Personuppgifter hänförliga till den Personuppgiftsansvariges patienter, inklusive hälsorelaterade och potentiellt känsliga uppgifter; och Personnummer Sjukfrånvaro/frånvaro Patientuppgifter

3) Här ska framgå om särskilda kategorier av personuppgifter enligt (definierat i art 9 p 1 Dataskyddsförordningen) ingår i behandlingen eller om det förekommer andra personuppgifter som är särskilt skyddsvärda. t.ex. Journalhandlingar i form av remiss, anamnes, bilder och svar.

4) Här ska kategorier av registrerade framgå. t.ex. Kategorierna av registrerade inkluderar: Patientuppgifter såsom remiss, anamnes, bilder och svar.

5) Specificera om personuppgifter kommer att överföras utanför EU/EES i anledning av tjänsten.

T.ex. Som en del av PUB:s fullgörande av tjänsterna som levereras enligt Tjänsteavtalet kan oidentifierade personuppgifter relaterade till supportärenden samt personuppgifter i form av kontaktuppgifter såsom namn, telefonnummer och e-postadress hänförliga till den PUA:s personal komma att föras över till PUB:s underleverantör, se Bilaga X.

6) PUB kommer att arbeta tillsammans med PUA för att bestämma gallringstiderna för Personuppgifter.

7) Eventuella instruktioner om hur återlämning av personuppgifter och annan data ska ske, se punkten 9.3. i detta Biträdesavtal.

8) Eventuella specifika krav av avser Informationssäkerhet eller IT-säkerhet. Detta kan vara redan specificerat i annan del av avtalet och en hänvisning kan vara tillräcklig.

9) Eventuella särskilda instruktioner kring behandling. Kan t.ex. avse att endast vissa individer får ha åtkomst till uppgifter. Att alla personuppgifter ska förvaras krypterade. Att vissa uppgifter ska beaktas särskilt (skyddade personuppgifter m.m.) eller om behandlingen av vissa uppgifter ska utföras på ett särskilt sätt eller endast under vissa förutsättningar. PUB får endast ha åtkomst till Personuppgifter i samband med ett supportärende som initierats av personal tillhörig PUA.

Praktisk hantering	
Fysisk säkerhet	Personuppgiftsbärande system ska skyddas mot elavbrott och andra störningar orsakade i tekniska försörjningssystem. Utrymmen där personuppgifter förvaras, så som serverhallar, ska skyddas genom lämpliga tillträdeskontroller för att säkerställa att endast behörig personal får tillträde. Det ska också finnas ett tillfredställande skydd mot stöld och händelser som kan förstöra IT-system och lagringsmedia.
Autentisering/identifiering	PUB ska se till att endast behörig personal kan komma åt personuppgifterna genom att skydda personuppgifterna med rätt identifiering. Personalen ska instrueras att hantera och förvara användaridentitet och lösenord med försiktighet och att använda lösenord som inte har anknytning till person eller på annat sätt som med lätthet kan forceras. Lösenord ska bytas regelbundet och personalen ska logga ut från sina respektive klientdatorer när de inte används
Behörighetskontroll	Ett tekniskt system för behörighetskontroll ska styra åtkomsten till personuppgifterna för PUB. 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.
Åtkomstskydd	När datorutrustning och löstagbara datamedier hos PUB 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.
Skadlig kod	Personuppgiftsbärande system ska vara skyddade mot virus, trojaner och andra former av digitala intrång.
Bärbara datorer	För det fall eventuella bärbara datorer används vid behandlingen ska personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.
Säkerhetskopia	Personuppgifterna ska regelbundet överföras till säkerhetskopior. Kopiorna ska förvaras avskilt och väl skyddade så att personuppgifterna kan återskapas efter en störning. PUB ska ha en rutin för test av återläsning.
Loggning	Åtkomst till personuppgifter ska kunna följas upp i efterhand genom en logg eller liknande underlag. Av loggarna ska det framgå vilka åtgärder som har vidtagits och vilka personuppgifter det gäller. Det ska också framgå när åtgärden har vidtagits och av vem. Underlaget ska kunna kontrolleras av PUB och återrapporteras till PUA.
Datakommunikation	PUB ska se till att PUB:s informationssystem är skyddade från extern åtkomst genom exempelvis perimeterskydd och kontroll av fjärråtkomst vid extern access. Insynsskydd ska tillföras transport och lagring när behovet finns.
PUB:s åtkomst till personuppgifter via fjärrstyrd datakommunikation	Service via fjärrstyrd datakommunikation får endast ske efter säker elektronisk identifiering av den som utför servicen. Servicepersonal ska ges åtkomst i systemet endast vid servicetillfället. Finns separat kommunikationsingång för service ska den vara stängd när service inte pågår.
Känsliga personuppgifter	För åtkomst till känsliga och integritetskänsliga personuppgifter krävs tvåfaktorsautentisering till tjänsten.

Överföring av personuppgifter	Personuppgifter som överförs via datorkommunikation utanför lokaler som kontrolleras av PUB ska skyddas med kryptering.
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 PUA:s personuppgifter, utförs av annan än PUB, ska kontrakt som reglerar säkerhet och sekretess träffas med serviceföretaget.
Servicebesök	Vid servicebesök ska servicen ske under PUB:s överinseende. Är detta inte möjligt ska lagringsmedier som innehåller personuppgifter avlägsnas.
Kontroll	PUA har rätt att utföra kontroller av att avtalade säkerhetsåtgärder faktiskt vidtas eller att kontrollen sker av oberoende part.
Obehörig åtkomst	PUA har rätt att utreda obehörig åtkomst hos PUB.

BILAGA 2 Lista över underleverantörer

1	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	
2	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	
3	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	
4	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	
5	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	

6	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	
7	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	
8	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	
9	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	
10	Namn och geografisk belägenhet	
	Personuppgifter som behandlas	
	Roll i dataprocessen	