Region Västmanland

# PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679[1]

## 1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

| **Personuppgiftsansvarig** | **Personuppgiftsbiträde** |
|---|---|
| *Region Västmanland* | Sectra Sverige AB |
| **Organisationsnummer** | **Organisationsnummer** |
| *232100-0172* | 556483-9479 |
| **Postadress** | **Postadress** |
| *Regionhuset, 721 89 Västerås* | Sectra Sverige AB<br>Teknikringen 20<br>583 30 Linköping |
| **Kontaktperson för administration av detta personuppgiftsbiträdesavtal** | **Kontaktperson för administration av detta personuppgiftsbiträdesavtal** |
| Namn: Mathias Hansson<br>E-post:mathias.hansson@regionvastmanland.se<br>Tfn: 021-176252 | Namn: Mikael Widén<br>E-post: mikael.widen@sectra.se<br>Tfn: 0705-275634 |
| **Kontaktperson för parternas samarbete om dataskydd** | **Kontaktpersoner för parternas samarbete om dataskydd** |
| Namn: Moon Carlbring<br>E-post: moon.carlbrig@regionvastmanland.se<br>Tfn: 021-176569 | Namn: Johan Åtting<br>E-post: dpo@sectra.se<br>Tfn: 0703-175232 |
| Personuppgiftsbiträdesavtal gäller för följande affärsavtal | |
| Service- och utvecklingsavtal gällande Sectra RIS och PACS (DOC-OANN-7ARJV7). | |

[1] Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbiträdets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.

## 2. DEFINITIONER

Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

| | |
|---|---|
| Behandling | En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. |
| Dataskyddslagstiftning | Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den Behandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning. |
| Personuppgiftsansvarig | Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter. |
| Instruktion | De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen. |
| Logg | Logg är resultatet av Loggning. |
| Loggning | Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person. |
| Personuppgiftsbiträde | Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning. |
| Personuppgift | 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 online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. |
| Personuppgiftsincident | 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 eller på annat sätt Behandlats. |
| Registrerad | Fysisk person vars Personuppgifter Behandlas. |
| Tredje land | En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES). |

| | |
|---|---|
| Underbiträde | Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning. |

## 3. BAKGRUND OCH SYFTE

3.1 Med detta Personuppgiftsbiträdesavtal jämte Instruktioner och en eventuell förteckning över Underbiträden (nedan gemensamt "PUB-avtalet") reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad stadgas i artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679 ("Dataskyddsförordningen").

3.2 När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet "Huvudavtalet" i PUB-avtalet.

3.3 För det fall något av det som stadgas i punkterna 1, 16, 17, 18.2, 19–22 i PUB-avtalet regleras på annat sätt i Huvudavtalet ska Huvudavtalets reglering ha företräde.

3.4 Hänvisningar i PUB-avtalet till nationell eller unionsrättslig lagstiftning, avser vid var tid tillämpliga bestämmelser.

## 4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

4.2 Den Personuppgiftsansvarige ska ge skriftliga Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.

4.3. Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

## 5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner så att Personuppgiftsbiträdet och eventuellt Underbiträde kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Huvudavtal i förekommande fall.

5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.

5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

## 6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet, Instruktioner och Dataskyddslagstiftningen.

6.3 Personuppgiftsbiträdet åtar sig att säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 i Dataskyddsförordningen fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap. III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.

6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner.

6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.

## 7. SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Dataskyddslagstiftningen för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.

7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.

7.4 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbiträdets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet.

## 8. SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, såvida inte annat avtalats.

8.2. Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.

8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.

8.4 Om den Registrerade, tillsynsmyndighet eller tredje man begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas. Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

## 9. GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål som en del av sina garantier, enligt artikel 28.1 i Dataskyddsförordningen, på den Personuppgiftsansvariges begäran kunna redovisa vilka tekniska och organisatoriska säkerhetsåtgärder som används för att Behandlingen ska uppfylla kraven enligt PUB-avtalet och artikel 28.3.h i Dataskyddsförordningen.

9.2 Personuppgiftsbiträdet ska minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.

9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska Personuppgiftsbiträdets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2–9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

9.5 Personuppgiftbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.

9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt punkten 9 i PUB-avtalet.

## 10. HANTERING AV RÄTTELSER OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbiträdets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella Personuppgiften som ett led i processen för rättelse eller radering.

10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan väntas påverka Behandlingen, ska Personuppgiftsbiträdet skriftligt informera den Personuppgiftsansvarige om detta i enlighet med vad stadgas om meddelanden i punkten 19 i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

## 11. PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt artikel 32.1.c i Dataskyddsförordningen.

11.2 Personuppgiftbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftbiträdet ska på

den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörigs Behandling och/eller åtkomst till Personuppgifterna.

11.3 Vid Personuppgiftsincident, vilken Personuppgiftbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå, tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

Beskrivningen ska redogöra för:

1. Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
2. de sannolika konsekvenserna av Personuppgiftsincidenten, och
3. åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftincidentens potentiella negativa effekter.

11.4 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkten 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

## 12. UNDERBITRÄDE

12.1 Personuppgiftsbiträdet äger rätt att anlita den eller de Underbiträden som framgår av bilagd förteckning över Underbiträden.

12.2 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt avtal med Underbiträdet som reglerar Behandlingen som Underbiträdet utför å en Personuppgiftsansvariges vägnar samt att endast anlita Underbiträden som ger tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddsförordningen. I fråga om dataskydd ska avtalet ålägga Underbiträdet samma skyldigheter som åläggs Personuppgiftsbiträdet i detta PUB-avtal.

12.3 Personuppgiftsbiträdet ansvarar fullt ut för Underbiträdets Behandling gentemot den Personuppgiftsansvarige.

12.4 Personuppgiftsbiträdet äger rätt att anlita nya underbiträden och ersätta befintliga underbiträden.

12.5 När Personuppgiftsbiträdet avser att anlita ett nytt eller ersätta ett befintligt Underbiträde ska Personuppgiftsbiträdet säkerställa Underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

1. Underbiträdets namn, organisationsnummer och säte (adress och land),
2. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
3. var Personuppgifterna ska behandlas.

12.6 Den Personuppgiftsansvarige äger rätt att inom trettio (30) dagar från dag för meddelande enligt punkten 12.5 invända mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde och att,

med anledning av sådan invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkten 17.4.

12.7 När Personuppgiftsbiträdet upphör med att anlita Underbiträdet ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om att det upphör med att anlita Underbiträdet.

12.8 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det avtal som reglerar Behandling av Underbiträdets Behandling av Personuppgifter enligt punkten 12.2.

## 13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.

13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.

13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkten 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

## 14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet, Instruktioner och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska artikel i 82 i Dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad sägs i Huvudavtalet gäller detta PUB-avtal, punkterna 14.1 och 14.2, före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser Behandlingen.

## 15. LAGVAL OCH TVISTLÖSNING

15.1 För detta avtal gäller svensk rätt. Eventuell tolkning eller tvist i anledning av PUB-avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol.

## 16. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

16.1 PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tillsvidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

## 17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

17.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.

17.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av båda parter.

17.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet och/eller Instruktioner ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.

17.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkten 12.6, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan.

## 18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

18.1 Vid uppsägning av PUB-avtalet ska den Personuppgiftsansvarige utan onödigt dröjsmål begära att Personuppgiftsbiträdet överlämnar samtliga Personuppgifter till den Personuppgiftsansvarige eller raderar dem, enligt dennes önskemål. Om Personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga Personuppgifter avses alla Personuppgifter vilka har omfattats av Behandlingen samt annan tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

18.2 Överlämning och radering enligt PUB-avtalet, punkten 18.1, ska vara utförda senast trettio (30) dagar räknat från den tidpunkt uppsägning gjorts enligt detta PUB-avtal, punkten 16.1.

18.3 Behandling som utförs av Personuppgiftsbiträdet efter den tidpunkt som stadgas i punkten 18.2 är att betrakta som en otillåten Behandling.

18.4 Bestämmelser om sekretess/tystnadsplikt i punkten 8 enligt detta PUB-avtal ska fortsätta gälla även om PUB-avtalet i övrigt upphör av gälla.

## 19. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

19.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas till respektive parts kontaktperson för PUB-avtalet.

19.2 Meddelanden om parternas samarbete om dataskydd, gällande Behandlingen, ska skickas till respektive parts kontaktperson för parternas samarbete om dataskydd.

19.3 Meddelanden inom ramen för PUB-avtalet och Instruktioner ska skickas skriftligt. Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

## 20. KONTAKTPERSONER

20.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.

20.2 Parterna ska utse var sin kontaktperson för parternas samarbete om dataskydd.

## 21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

21.1 Varje part ansvarar för att de uppgifter som anges i punkten 1 i PUB-avtalet alltid är aktuella. Ändring av uppgifter i punkten 1 ska meddelas skriftligen enligt punkten 19.1 i PUB-avtalet.

## 22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt tecknande eller i pappersformat för tecknande med penna. Om PUB-avtalet tillhandahålls i digitalt format utgår punkter 22.2–22.3.

22.2 Den Personuppgiftsansvarigés undertecknande av PUB-avtalet

Ort Datum

Västerås 16/5 24

.....

*Undertecknande*

.....

*Namnförtydligande*

22.3 Personuppgiftsbiträdets undertecknande av PUB-avtalet

Ort Datum

Linköping 2024-05-06

.....

*Undertecknande* Dominica D-Lilliestråle

.....

*Namnförtydligande* Dominica D-Lilliestråle

## Bilaga 1. Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående Instruktion:

| **1. Ändamål, föremålet och arten** |
|---|
| Personuppgiftsbiträdet (PuB) behandlar personuppgifter för personuppgiftsansvarigs (PuA) räkning i syfte att tillhandahålla och leverera tjänsterna i enlighet med sina åtagande utifrån huvudavtalet, "Service och utvecklingsavtal" (DOC-OANN-7ARJV7-1.0). Tjänsterna omfattar övervakning och underhåll av kärnsystemen RIS/PACS/VNA för lagring av medicinsk multimedia med tillhörande patientinformation såsom remissinformation och journalanteckningar samt även tillhandahållande av support avseende detta system. För vissa tilläggstjänster innefattas även drift utanför PUAs driftsmiljö. Därutöver behandlar personuppgiftsbiträdet Region Västmanlands anställdas kontaktuppgifter i samband med supportärenden. |
| **2. Behandlingen omfattar följande typer av Personuppgifter** |
| Personuppgifter bestående av medicinska bilder, personnummer, namn, adress, journaltext, remisstext, röntgenutlåtande, loggar. Behandlingen kan även omfatta kontaktuppgifter för PUA:s personal samt de personuppgifter som PUA lagrar i systemet. |
| **3. Behandlingen omfattar kategorier av Registrerade** |
| Behandlingen omfattar PUA:s medarbetare samt patienter från regionen eller andra vårdgivare som är anslutna via sammanhållen journal. |
| **4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena** |
| Utifrån affärsavtalet där kontinuerlig övervakning av systemets prestanda ingår har leverantören access till systemkomponenter hos PUA som inkluderas i den tekniska driftlösningen. Inloggning till PUAs driftmiljö ska ske på ett säkert och sätt enligt region Västmanlands rutiner för insläpp.<br><br>PuB ska på anmodan redovisa sin rutin för gallring och radering av data för att säkerställa att personuppgifter hanteras på ett adekvat sätt enligt gällande lagstiftning. Personuppgifter från Region Västmanland ska sparas separerat från andra personuppgiftsansvarigas data. |
| **5. Ange särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena** |
| Organisatoriska och tekniska säkerhetsåtgärder ska lyda minst men inte begränsas till följande:<br><br>• Personuppgiftsbiträdet ska säkerställa att personuppgifter behandlas enbart i enlighet med Personuppgiftsansvariges instruktion.<br><br>• Personuppgiftsbiträdet ska ha ett ledningssystem för informationssäkerhet.<br><br>• Personuppgiftsbiträdet ska vidta tekniska och organisatoriska åtgärder som förhindrar obehörigt tillträde och skadlig inverkan på personuppgifter och system där personuppgifter behandlas. Personuppgiftsbärande system ska skyddas mot elavbrott och andra störningar orsakade i tekniska försörjningsystem. 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. 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.

- Personuppgiftsbiträdet ska ha en effektiv behörighetsstyrning. Personal med behörighet till personuppgiftsansvariges personuppgifter ska vara dokumenterade. Personuppgiftsbiträdet ska säkerställa att personer som har rätt att använda system för behandling av personuppgifter får åtkomst till sådana personuppgifter endast i den utsträckning de har rätt till, i enlighet med sina åtkomsträttigheter, och att det under behandlingen eller användningen och efter lagringen inte går att läsa, kopiera, ändra eller radera personuppgifter utan behörighet (kontroll av dataåtkomst).

- Personuppgiftsbiträdet 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. Personalen ska logga ut från sina respektive klientdatorer när de inte används.

- Personuppgiftsbiträdet ska ha ett tekniskt system för behörighetskontroll ska styra åtkomsten till personuppgifterna. 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. Om det är tillämplig ska Region Västmanland ha administratörsroll som möjliggör egen tilldelning och administrering av behörigheter.

- Åtkomst till känsliga personuppgifter ska föregås av stark autentisering.

- Personuppgiftsbiträdet ska ha ett arbetssätt som upptäcker och identifierar incidenter samt förankrade rutiner för incidentrapportering inom organisationen och till personuppgiftsansvarig.

- Personuppgiftsbiträdet ska ha ett etablerat arbetssätt för riskhanteringar.

- Personuppgiftsbiträdet ska på begäran av personuppgiftsansvarige och/eller 3 månader efter avslutat supportärende radera samtliga personuppgifter och tillhörande kontouppgifter. Personuppgiftsbiträdet får behålla och behandla Personuppgifter utan hinder av detta PUB-avtal om det krävs av Personuppgiftsbiträdet för att Personuppgiftsbiträdet ska kunna uppfylla sina rättsliga förpliktelser (det vill säga om unionsrätten eller nationell rätt kräver fortsatt lagring, exempelvis med anledning av redovisningsskyldighet). Vid affärsavtals upphörande åligger det leverantören att informera PUA och kontaktpersonen för detta avtal om vilka uppgifter som är aktuella utifrån ovan skrivelse.

- Personuppgiftsbiträdet ska tillse att samtliga data som samlas in, överförs och lagras ska vara krypterad. Krypteringsprotokoll ska vara standardiserad som lägst enligt TLS 1.3/AES256 eller annan motsvarande krypteringsprotokoll som skriftligt godkänns av Region Västmanland.

- Personuppgiftsbiträdet ska upprätthålla tekniskt underhåll för att tillhandahålla den tjänst och utrustning som den Personuppgiftsansvarige använder. Personuppgiftsbiträdet ska säkerställa att personuppgifter skyddas mot oavsiktlig förstöring eller förlust samt för vissa tilläggstjänster säkerställa säkerhetskopiering och kontinuitet (tillgänglighetskontroll).

- Leverantören ska ha en inbyggd funktion för automatisk utloggning efter 10 minuters inaktivitet.

- Personuppgiftsbärande system ska vara skyddade mot virus, trojaner och andra former av digitala intrång.

- Personuppgiftsbiträdet ska säkerställa att region Västmanlands data är skyddade från extern åtkomst genom exempelvis perimeterskydd och kontroll av fjärråtkomst vid extern access.

- Personuppgiftsbiträdet ska säkerställa att service och support via fjärrstyrd datakommunikation endast sker 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.

- Personuppgiftsbiträdet ska vid avtalets upphörande efter överenskommelse återlämna aktuell data för tilläggstjänster som driftas utanför PUA´s driftsmiljö i standardiserade öppna format som Region Västmanland bedömer vara läsbart.

**Rapportering av personuppgiftsincidenter**
PUB ska ha en rutin för rapportering och hantering av personuppgiftsincidenter och säkerhetsincidenter samt, efter upptäckt, rapportera utan onödigt dröjsmål till PUA genom att kontakta PUAs ansvarig för huvudavtalet eller dataskyddsombudet@regionvastmanland.se. Rapporten som förmedlas ska innehålla uppgifter om hur, vad, när, vilkas uppgifter och i vilken omfattning incidenten har skett samt vilka åtgärder som vidtagits.

**6. Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem**

Åtkomst till personuppgifter för PuBs medarbetare ska styras av ett tekniskt system för behörighetskontroll. Medarbetarna ska ges minsta möjliga åtkomst vid behandling av Personuppgifter. Endast medarbetare som behöver tillgång till Personuppgifter för sitt arbete ska ges åtkomst. Det ska finnas dokumenterade rutiner för tilldelning och borttagande av behörigheter.

Åtkomst till Personuppgifter ska kunna kontrolleras i efterhand genom loggar. Loggarna ska kontrolleras regelbundet i syfte att upptäcka otillåten eller obehörig tillgång till personuppgifter och innehålla tidpunkt, vem som läser, registrerar, ändrar, tar bort data.
Rutiner/processer/metoder för hantering av information i transaktionslogg och systemlogg ska finnas (då dessa kan innehålla känsliga personuppgifter). Där det är möjligt, bör inte systemadministratörer ha behörighet att radera och avaktivera loggar över sina egna aktiviteter.

Loggningen ska redogöra tid enligt UTC +1, datum, unik och personlig identifikator samt samtliga aktiviteter som inkluderar men inte begränsas till följande; vem som läst, raderad och redigerat.

**7. Lokalisering och överföring av Personuppgifter till Tredje land**

Inga tredjelandsöverföringar ska förekomma, vid de fall där det är absolut nödvändigt för att kunna utföra support ska det särskilt överenskommas med personuppgiftsansvarig och ett av nedanstående kriterier måste uppfyllas, dokumenteras och godkännas.

- Leverantören ska ha ett av Integritetsskyddsmyndigheten eller annan tillsynsmyndighet inom EU godkänt BCR (Binding corporate rules)

- Om leverantören är registrerad och lokaliserad i ett land som EU-kommissionen godkänt som ett land med adekvata skyddsnivå eller om det tecknats SCC (Standard contractual clauses som är framtagen av EU-kommissionen) med underbiträdet i samband med tredjelandsöverföring.

- Tredjelandsöverföring som uppkommer i samband med nyttjande av underbiträde ska biträdet tillse att lämpliga skyddsåtgärder vidtas enligt artikel 46 allmänna dataskyddsförordningen och enligt EDPBs riktlinjer om säkerhetsåtgärder.

- Tredjelandsöverföring till USA som av EU-kommissionen har bedömts ha adekvat skyddsnivå enligt artikel 45 ska vara anslutna och certifierade mot Data Privacy Framework.

**8. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av biträdet/biträdena**

Vid utökning eller införande med behandling av ny eller innovativ teknik så som AI funktionalitet eller annan liknande automatiserad teknik/funktion skall detta regleras genom separat instruktion som särskilt beaktar den nya AI förordningen (AI- Act)

## Bilaga 2. Personuppgiftsbiträdets biträdesförhållande vid avtalstecknandet.

Biträdet ska vid de fall det är aktuellt ange ifall personuppgiftsbiträdet ingår i en koncern, om ja redogör bolagsuppgifter för koncernen.

Biträdet ska vid de fall det är aktuellt ange vilka underbiträden bolaget anlitar som kommer behandla eller ta del av personuppgiftsansvariges personuppgifter.

Inom parentes anges de länder där respektive bolag är etablerat och från vilka personal kan komma att behandla personuppgifter.

Behandla supportärenden, samtal och andra supportförfrågningar från den personuppgiftsansvarige.

| ☐ | Det finns inga underleverantörer vid avtalets ingående | |
|---|---|---|
| 1 | **Namn och geografisk belägenhet** | **Sectra Imaging IT Solutions AB, Sverige** |
| | Personuppgifter som behandlas | Patientuppgifter, t.ex. namn, personnummer, medicinska bilder, undersökningsnummer, remissnummer samt relaterad information.<br><br>Användaruppgifter, t.ex. namn, roll och avdelning samt uppgifter om systemanvändning och audit loggning. |
| | Roll i dataprocessen | Tillhandahåller support, eskalerad produktsupport, service och uppgraderingar på de produkter inom medicinsk bild och bilddiagnostik som Sectra Sverige AB levererar till Region Västmanland. |
| 2 | **Namn och geografisk belägenhet** | **Sectra AB, Sverige** |
| | Personuppgifter som behandlas | Patientuppgifter, t.ex. namn, personnummer, medicinska bilder, undersökningsnummer, remissnummer samt relaterad information.<br><br>Användaruppgifter, t.ex. namn, roll och avdelning samt uppgifter om systemanvändning och audit loggning. |
| | Roll i dataprocessen | Tillhandahåller infrastruktur- och driftstjänster till Sectra-koncernen, exempelvis systemstöd för support, nätverksanslutningar via Sjunet , som krävs för att möjliggöra service och support på de produkter inom medicinsk bild och bilddiagnostik som Sectra Sverige AB levererar till Region Västmanland. |
| 3 | **Namn och geografisk belägenhet** | **Sectra Ltd, Sectra Products Ltd, UK** |
| | Personuppgifter som behandlas | Patientuppgifter, t.ex. namn, personnummer, medicinska bilder, undersökningsnummer, remissnummer samt relaterad information.<br><br>Användaruppgifter, t.ex. namn, roll och avdelning samt uppgifter om systemanvändning och audit loggning. |
| | Roll i dataprocessen | Installation, utbildning och support av Analytics.<br><br>Fjärrsupport för DoseTrack och IEP, i de fall första och andra linjens support i Sverige ej klarar av att lösa uppgiften. |

| Versionshantering | | | | |
|---|---|---|---|---|
| Dokument | Version | Datum | Ändringar | Ansvarig |
| Avtal | 1.2.1 | 2020-01-02 | 17.4 | PR (SKR) |
| Bilaga 1 | 1.2 | 2019-10-25 | Borttag av 'Mall för förteckning över Underbiträden vid PUB-avtalets ingående | PR (SKR) |
| Bilaga 2 | 1.1 | 2021-05-05 | Tillägg, Biträdesförhållanden Redogör ifall biträdet ingår i en koncern | MC (RV) |