Karolinskas Diarienummer

Bilaga 11 - Personuppgiftsbiträdesavtal

Parter

1.1 Personuppgiftsansvarig (PuA):

1.2 Personuppgiftsbiträde (PuB): Karolinska Universitetssjukhuset(org.nr:232100–0016)

2. Definitioner

2.1 Med "Avtalet" avses huvudavtalet till vilket denna Bilaga är bifogad.

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

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

2.4 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.

3. Bakgrund och syfte

3.1 PuA har beslutat att använda Regionerna Stockholm och Gotlands Vårdinformationssystem enligt de regler och villkor som framgår av Avtalet i övrigt.. Samarbetet/tjänsterna innebär att PuB behandlar Personuppgifterna för PuA:s räkning.

[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

3.2 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.

4. Omfattning

4.1 Föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade framgår av ifylld Instruktion/ specifikation till Personuppgiftsbiträdesavtal (bilaga A härtill).

4.2 Eventuella ändringar i PuA:s instruktioner ska förhandlas separat och ska, för att bli gällande, dokumenteras skriftligt och undertecknas av båda parterna, med undantag för sådana instruktioner som PuA ska ha rätt att lämna på grund av ändringar i Tillämplig dataskyddslag.

5. PuA:s ansvar

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

5.2 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 denna Bilaga.

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

6. PuB:s allmänna åtaganden

6.1 PuB åtar sig, i sin egenskap av PuB, att endast behandla Personuppgifterna för att fullgöra sina uppgifter enligt denna Bilaga och endast på sätt som framgår av Bilagan och/eller PuA:s skriftliga instruktioner.

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

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

6.4 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.

6.5 För det fall det skulle finnas behandlingar som PuB enligt tvingande lag måste utföra utöver de dokumenterade instruktioner som lämnats av PuA, ska PuB underrätta PuA innan sådan behandling påbörjas, om det inte föreligger hinder mot att lämna sådan underrättelse enligt tvingande lag.

6.6 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.

7. Säkerhet och sekretess

7.1 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 artikel 32.

7.2 Eventuella särskilda krav på säkerhetsåtgärder framgår av ifylld Instruktion/ specifikation till Personuppgiftsbiträdesavtal (bilaga A härtill).

7.3 Vidtagna säkerhetsåtgärder ska dokumenteras.

7.4 Dokumentationen enligt föregående punkt ska, för det fall det inte riskerar informationssäkerheten avseende Personuppgifterna eller utgör PuB:s företagshemligheter, på begäran tillhandahållas PuA.

7.5 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.

7.6 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.

8. De registrerades rättigheter

8.1 PuB åtar sig att i den mån detta är möjligt bistå PuA genom lämpliga tekniska åtgärder vad gäller begäran från registrerade om att utöva deras rättigheter enligt Tillämplig dataskyddslag, exempelvis rättelse, radering eller begränsning av behandling.

8.2 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.

9. Revision, insyn och tillsyn

9.1 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.

9.2 PuB ska tillåta och möjliggöra de inspektioner som Integritetsskyddsmyndigheten 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.

9.3 PuB ska tillåta och möjliggöra de revisioner som 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.

9.4 PuA ska bära kostnaderna för revision och ska inte åsamka störningar som påverkar PuB:s förvaltning av Regionerna Stockholm och Gotlands Vårdinformationssystem.

10. Personuppgiftsincidenter

10.1 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 artikel 4).

10.2 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 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.

10.3 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.

11. Överföring av personuppgifter till tredje land

11.1 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 parterna kommer överens om något annat.

11.2 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.

11.3 Överföring till Tredje land för Behandling enligt punkten 11.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i denna Bilaga och dess instruktioner.

12. Anlitande av annat personuppgiftsbiträde

12.1 PuA godkänner att PuB får anlita underbiträden inom EU/EES. Om PuB avser att anlita ett nytt eller ersätta ett befintligt underbiträde för att behandla personuppgifter som omfattas av detta avtal ska PuB i förväg informera PuA om detta och bereda denne möjlighet att framföra invändningar. Sådana invändningar ska ske skriftligen inom fjorton (14) dagar från det att PuA fått informationen. Om PuA invänder mot de ändringar som PuB informerat om i enlighet med denna punkt har PuB rätt att inom trettio (30) dagar från invändningen säga upp hela eller de delar av Avtalet som PuB inte kan tillhandahålla utan användning av underbiträdet som PuA invänt emot.

12.2 PuB:s skyldighet att informera PuA i enlighet med föregående punkt fullgörs genom överenskommen kontaktväg. Informationen ska innehålla uppgift om underbiträdets bolagsnamn, adress, berörda personuppgiftsansvariga och typ av behandling.

12.3 Om PuB anlitar annat personuppgiftsbiträde enligt p.12.1, 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.

12.4 Om PuB anlitar annat personuppgiftsbiträde enligt p. 12.1, ansvarar PuB för att det andra personuppgiftsbiträdet fullgör alla åtaganden och iakttar alla begränsningar som anges i denna bilaga.

12.5 PuB ska vid var tid föra en korrekt och uppdaterad lista över personuppgiftsbiträden som anlitats enligt detta avsnitt. PuB:s underbiträdeslista finns tillgänglig på Leverantörens Webbsida (enligt definition i Bilaga 1 (Definitioner)).

13. Giltighetstid

13.1 Bestämmelserna i denna Bilaga ska gälla från och med Avtalets undertecknande och därefter så länge som PuB behandlar Personuppgifterna.

13.2 Åtagandena rörande sekretess och tystnadsplikt ska äga giltighet även sedan Avtalet i övrigt har upphört att gälla.

14. Upphörande av behandling av personuppgifter

14.1 Vid upphörande av PuB:s uppdrag gäller Bilaga 9 (Sammanhållen vård- och omsorgsdokumentation) till Avtalet.

14.2 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.

15. Ersättning

15.1 Om inte annat särskilt överenskommits har PuB rätt till skälig ersättning för fullgörande av sina skyldigheter i denna Bilaga om inte annat framgår av Avtalet i övrigt.

16. Skadeslöshet

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

17. Ändringar och tillägg

17.1 Ändringar av och tillägg till denna Bilaga ska vara skriftliga och undertecknade av behörig företrädare för båda parter.

18. Tvist

18.1 Tvist angående tolkning eller tillämpning av denna Bilaga hanteras enligt bestämmelserna om tvistelösning i Avtalet.

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

Behörig företrädare för PuA

Ort och datum

Namnförtydligande och titel

Behörig företrädare för PuB (dvs. verksamhetschef eller motsv.)

Solna

Ort och datum

Anders Hult
Verksamhetsområdeschef
Verksamhetsområde IT

Namnförtydligande och titel

Bilaga A - Instruktion/specifikation till Personuppgiftsbiträdesavtal

Utöver vad som redan framgår av personuppgiftsbiträdesavtalet 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.).

Generell instruktion

Beskriv **ändamålen** med PuB:s behandling av personuppgifter. Beskriv varför PuB behandlar uppgifterna för PuA:s räkning. T.ex. administration av kundförhållande, löneadministration, lagring av PuAs information rörande [x].	Tillhandahålla IT-stöd för Vårdprocess och Läkemedelsprocess i Region Stockholm och Region Gotland till Vårdgivare. Verkställa datautag enligt separat beslut och instruktion från PuA. Vid behov verkställa behörighetstilldelningar enligt separat beslut och instruktion från PuA.
Ange vilka **kategorier av personuppgifter** som kommer behandlas av PuB. T.ex. namn, adress, e-post, kundnummer, personnummer, vårddokumentation, löneuppgifter.	**Patienter:** Namn, adress, epost, telefonnummer, personnummer, Vårddokumentation mm som behövs för att bedriva Hälso- och Sjukvård och rapportering av det. **Anställda:** Namn, adress, epost, telefonnummer, personnummer, HSAID
Ange samtliga **kategorier av registrerade** vars uppgifter kommer behandlas av PuB. T.ex. patienter, kunder, kontaktpersoner hos leverantörer eller konsulter, anställda.	Patienter, anställda.
Ange **vilka behandlingar** som kommer utföras av PuB och	Lagring, drift, behörighets admin, felsökning support. PuB kan komma att ha åtkomst till patient- och personaldata vid service men det ingår inte i aktiviteterna att behandla dessa

behandlingens karaktär. Beskriv behandlingsaktiviteter som t.ex. lagring, administrering, samkörning av register. Ange vidare om behandlingen t.ex. rör stora mängder data eller om behandlingen innefattar profilering.	
Beskriv **hur länge** behandlingen kommer att pågå. Om perioden inte går att fastställa, ange vilka parametrar som ligger till grund för bedömningen av tidsperioden (t.ex. eventuellt huvudavtals löptid).	PuB ska behandla uppgifterna fram tills att PuA informerar PuB om att behandlingen ska upphöra, om inte något annat särskilt har avtalats.
Ange **tidsfrist för radering** och eventuell **återföring** av personuppgifter vid avtalets upphörande.	Vid upphörande av uppdrag ska PuA instruera PuB hur data ska hanteras i enlighet med Bilaga 9 (Sammanhållen vård- och omsorgsdokumentation).
Kontaktväg för information Ange kontaktväg PuB ska använda för att skicka information som PuB är skyldiga att informera PuA .	PuB publicerar information på: Avtal - Vårdinformationssystem https://vardinformationssystem.regionstockholm.se/huvudjournalsystemet-take-care/tjanster-och-avtal/avtal/

Ska personuppgifter överföras till tredje land (land utanför EU/EES) eller internationell organisation?

JA ☐ NEJ ☐

Om JA:

Överföring av personuppgifter till tredje land eller internationell organisation är tillåten endast om en eller flera av de grunder för överföring som framgår nedan är uppfyllda (kryssa i en eller flera):

EU-kommissionen har beslutat att det aktuella mottagarlandet säkerställer en adekvat skyddsnivå (**artikel 45** dataskyddsförordningen)	☐
Lämpliga skyddsåtgärder har vidtagits och lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga (**artikel 46** dataskyddsförordningen), t.ex. genom upprättande av EU-kommissionens standardavtalsklausuler samt eventuella ytterligare vidtagna säkerhetsåtgärder.	☐
Överföringen är nödvändig av viktiga skäl som rör allmänintresset (**artikel 49.1 d** dataskyddsförordningen). Kräver lagstöd i nationell rätt eller EU-rätt.	☐
Överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke (**artikel 49.1 f** dataskyddsförordningen).	☐
Överföringen görs från ett register som enligt unionsrätten eller svensk rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, men endast i den utsträckning som de i unionsrätten eller i svensk rätt angivna villkoren uppfylls i det enskilda fallet (**artikel 49.1 g** dataskyddsförordningen).	☐

Tekniska eller organisatoriska säkerhetsåtgärder

Som framgår av personuppgiftsavtalet är PuB skyldig att 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, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Oaktat PuBs ansvar enligt ovan och vad som följer av PUB-avtalet samt Dataskyddsförordningen, ska PuBs tekniska och organisatoriska säkerhetsåtgärder omfatta följande:

Fysisk åtkomstkontroll Beskriv krav på åtgärder som förhindrar obehörigas fysiska tillgång till IT-system där behandlingen av personuppgifter sker.	I enlighet med Region Stockholms policys och riktlinjer.
Åtkomstkontroll avseende IT-system Beskriv krav på åtgärder som förhindrar obehöriga att använda IT-system.	Tvåfaktor-autentisering med DIGG-godkänd lösning för LOA3
Åtkomstkontroll avseende personuppgifter Beskriv krav på åtgärder för att säkerställa att personer som är behöriga att använda IT-systemet endast bereds tillgång till personuppgifter som omfattas av personernas fastställda behörighet.	Personlig behörighetstilldelning i systemen. Behörigheter revideras kontinuerligt. Behörighetsnivåer för olika typer av uppdrag finns. Pubs administrativa personals accesser loggas i systemet och följs upp i loggranskningsverktyget SALA månadsvis
Intrångsskydd Beskriv bl.a. krav avseende intrångsskydd mot skadlig kod och detektering av skadlig kod.	Brandväggar, virusskydd, checksummekontroll på klienter.
Lagringsregler Beskriv krav på åtgärder för att tillse att personuppgifter gallras under och efter avtalstiden när användningen inte längre är nödvändig för det ursprungliga ändamålet. Obs gallring / radering omfattar både skarpa miljöer och säkerhetskopior.	Ingen gallring sker annat än på direkta uppdrag från PuA
Säkerhetskopiering Beskriv krav avseende rutiner för säkerhetskopiering av information	Back-up är sekundär återställningsmetod. Normalt bör systemet återställas från snapshot och transloggar. Klassisk backup tas och sparas i 10 år
Kontinuitetsplanering och katastrofberedskap Beskriv krav på kontinuitetshantering och katastrofberedskap, inklusive ev. krav på redundans och åtgärdstider vid katastrof.	Redundanta driftshallar med hot-standby. Återställningstid <2 timmar. Läskopia görs tillgänglig omedelbart vid ett eventuellt avbrott på huvudservers. Finns möjlighet för PuA att ha lokal kopia på akutliggare och läkemedelslista för inneliggande patienter. Ansvaret att ha reservrutiner för verksamheten ligger på PuA.
Funktioner och rutiner för incidentrapportering Beskriv krav på åtgärder i samband med incidenter, utöver vad som framgår av PUB-avtalet, i syfte att ansvarige ska kunna fullgöra sina rapporteringsskyldigheter vid incident till DI respektive i förekommande fall registrerade. T.ex. hänvisa till PuA:s incidentrapporteringsrutin.	Information om personuppgiftsincidenter distribueras via epostlistan Vårdgivarspecifika förvaltningar som når respektive PuAs supportorganisation.

Ytterligare instruktioner som PuB måste beakta vid behandling av personuppgifter för PuA:s räkning: