

Bilaga 1 - Instruktion/specifikation till Personuppgiftsbiträdesavtal

Utöver vad som redan framgår av personuppgiftsbiträdesavtalet ska PuB följa nedanstående instruktioner.

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].

- *PuB förvarar personuppgifter åt PuA*

Ange vilka kategorier av personuppgifter som kommer behandlas av PuB:

T.ex. namn, adress, e-post, kundnummer, personnummer, vårddokumentation, löneuppgifter.

- *Personuppgifter såsom namn, kontaktuppgifter, personnummer och vårddokumentation som registreras i PuAs patientjournaler samt personuppgifter som registreras vid support*

Ange samtliga kategorier av registrerade vars uppgifter kommer behandlas av PuB:

T.ex. patienter, kunder, kontaktpersoner hos leverantörer eller konsulter, anställda.

- *Patienter samt till PuA knutna användare (anställda och inhyrda) av Region Stockholms Take Care-installation*

Ange vilka behandlingar som kommer utföras av PuB och 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.

- *Lagring och bearbetning*

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).

- *Tillsvidare*

Region Stockholm

Postadress:
FSTC, Stab Vårdstöd
Princeton, plan 5
171 76 Stockholm

Besöksadress:
FSTC, Stab Vårdstöd
Eugeniavägen 18, plan 5
171 64 Solna

Säte: Stockholm
Org nr: 232100-0016

Ange tidsfrist för radering och eventuell återföring av personuppgifter vid avtalets upphörande:

Ange ev. kvalificering av tidsfrist inom vilken PuB ska vara skyldig att radera personuppgifterna efter att avtalet/uppdraget har upphört. Ange också ev. tidsfrist inom vilken PuB ska återföra alla personuppgifter till PuA (och i förekommande fall, i vilket format), om sådan återföring ska ske.

- *Gallring enligt Arkivmyndighetens regler*

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):

- *Överföringen sker till annat land inom EU/EES eller till tredje land eller internationell organisation som av EU-kommissionen har bedömts ha en adekvat skyddsnivå.*

Tekniska eller organisatoriska säkerhetsåtgärder

Som framgår av PUB-avtalet 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 PuB:s 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.

- *Ja enligt Region Stockholms policy och riktlinjer*

Åtkomstkontroll avseende ITsystem:

Beskriv krav på åtgärder som förhindrar obehöriga att använda IT-system.

- *Ja tvåfaktorsautentisering krävs.*

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.

- *Stöds enligt enligt PDL:s krav*

Intrångsskydd:

Beskriv bl.a. krav avseende intrångsskydd mot skadlig kod och detektering av skadlig kod.

- *Ja. Krav finns.*

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.

- Ja. Stödjer PDL och GDPR.

Kryptering och pseudonymisering:

Beskriv krav på kryptering och/eller pseudonymisering i samband med hantering av uppgifterna, utöver vad som beskrivits under "Åtkomstkontroll vid överföringar".

- All kommunikation mellan system är krypterad och säkrad av tvåfaktorsautentisering.

Säkerhetskopiering:

Beskriv krav avseende rutiner för säkerhetskopiering av information

- Backup rutiner finns och verifieras frekvent.

Kontinuitetsplanering och katastrofberedskap:

Beskriv krav på kontinuitetsplanering och katastrofberedskap, inklusive ev. krav på redundans och åtgärdstider vid katastrof.

- Varje vårdgivare ansvarar för egna kontinuitetsplaner för verksamheten i händelse av tekniskt haveri.
- Tekniska miljöer utformas för att stödja verksamheternas tillgänglighetskrav.

Implementerade säkerhetsföreskrifter:

Beskriv krav på interna säkerhetsföreskrifter som ska gälla för personuppgiftsbehandlingen.

- Behandling av personuppgifter vid Karolinska Universitetssjukhuset STAB5557

Certifieringar:

Beskriv krav på eventuella certifieringsmekanismer eller uppförandekoder för dataskydd som biträdet ska inneha eller har åtagit sig att följa.

- Krav på CE-märkning enligt läkemedelsverkets föreskrifter för medicintekniska produkter när dessa används.
- Krav på följsamhet till PDL

Funktioner och rutiner för incidentrapportering

Beskriv krav på åtgärder i samband med incidenter, utöver vad som framgår av PUBavtalet, i syfte att ansvariga ska kunna fullgöra sina rapporteringsskyldigheter vid incident till DI respektive i förekommande fall registrerade. T.ex. hänvisa till PuA:s incidentrapporteringsrutin.

- Varje PUA ansvarar för rapportering av personuppgiftsincidenter till DI.

Revisionsregler:

Beskriv ev. revisionsregler som avviker från vad som framgår av Bilaga 1, Personuppgiftsbiträdesvillkor. T.ex. att PuA kräver regelbundet tillhandahållande av bevis om tredjepartsrevision eller accepterar bevis om tredjepartsrevision som alternativ till revisionsreglerna i PUB-avtalet.

- - - - -

Godkända underbiträden

Fullständig lista över underbiträden som godkänts i samband med PUB-avtalets ingående. PuB ansvarar för att tabellen nedan utgör en fullständig sammanställning över samtliga godkända underbiträden.

UNDERBITRÄDE:

Organisationens namn och org.nr:

**CompuGroup Medical Sweden AB,
Organisationsnummer 556349-5893**

Adress och kontaktuppgifter:

Rättarvägen 3, 8 trappor, 169 68 STOCKHOLM

Kontaktperson (inkl. kontaktuppgifter):

Magnus Eckemark, tel 08 453 55 04

Avtalsdatum för underbiträdesavtal mellan PuB och underbiträdet:

Finns undertecknat

Beskrivning av tjänsten som underbiträdet tillhandahåller:

Underhåll, teknisk support och utveckling av TakeCare med stödsystem.

Var (geografiskt) kommer underbiträdet att behandla personuppgifterna:

Sverige

Vid överföring till tredje land eller internationell organisation, ange den rättsliga grunden (se avsnitt härom ovan):

Ej aktuellt

UNDERBITRÄDE:

Organisationens namn och org.nr

**Region Stockholm, Serviceförvaltningen,
Organisationsnummer 232100-0016**

Adress och kontaktuppgifter:

Serviceförvaltningen, Norra Stationsgatan 69, 113 64 STOCKHOLM

Kontaktperson (inkl. kontaktuppgifter):

Elena Zefirova, tel 08-123 177 41

Avtalsdatum för underbiträdesavtal mellan PuB och underbiträdet:

Finns undertecknat

Beskrivning av tjänsten som underbiträdet tillhandahåller:

Teknisk drift och teknisk applikationsförvaltning av Region Stockholms TakeCare-installation med sidosystem

Var (geografiskt) kommer underbiträdet att behandla personuppgifterna:

Sverige

Vid överföring till tredje land eller internationell organisation, ange den rättsliga grunden (se avsnitt härom ovan):

Ej aktuellt

UNDERBITRÄDE:

Organisationens namn och org.nr:

CSAM Sweden AB

Organisationsnummer 556569-8338

Adress och kontaktuppgifter:

Telegrafgatan 4, Solna

Kontaktperson (inkl. kontaktuppgifter):

Andreas Persson, +46 (0) 8640 9005

Avtalsdatum för underbiträdesavtal mellan PuB och underbiträdet:

Finns undertecknat

Beskrivning av tjänsten som underbiträdet tillhandahåller:

Teknisk support för Picsara (sidosystem till TakeCare i Region Stockholms TakeCare-installation)

Var (geografiskt) kommer underbiträdet att behandla personuppgifterna:

Sverige

Vid överföring till tredje land eller internationell organisation, ange den rättsliga grunden (se avsnitt härom ovan):

Ej aktuellt

UNDERBITRÄDE:

Organisationens namn och org.nr:

Omniq AB

Organisationsnummer 559030-4456

Adress och kontaktuppgifter:

Box 190, 101 23 Stockholm

Kontaktperson (inkl. kontaktuppgifter):

Martin Williamsson, tel 073-355 60 43.

Avtalsdatum för underbiträdesavtal mellan PuB och underbiträdet:

Finns undertecknat

Beskrivning av tjänsten som underbiträdet tillhandahåller:

Teknisk support, underhåll och vidareutveckling av sidosystem i Region Stockholms TakeCare-installation, som utvecklats av Omniq AB.

Var (geografiskt) kommer underbiträdet att behandla personuppgifterna:

Sverige

Vid överföring till tredje land eller internationell organisation, ange den rättsliga grunden (se avsnitt härom ovan):

Ej aktuellt

UNDERBITRÄDE:

Organisationens namn och org.nr:

Gisys AB

Organisationsnummer 556181-9532

Adress och kontaktuppgifter:

Vretenvägen 2, 171 54 SOLNA

Kontaktperson (inkl. kontaktuppgifter):

Robert Olsson tel vx 08-564 200 50

Avtalsdatum för underbiträdesavtal mellan PuB och underbiträdet:

Finns undertecknat

Beskrivning av tjänsten som underbiträdet tillhandahåller:

Programmering och tekniskt underhåll av kod som ägs av Region Stockholm och ingår i sidosystem till Region Stockholms TakeCare-installation, och utvecklats av Gisys AB på uppdrag av Region Stockholm.

Var (geografiskt) kommer underbiträdet att behandla personuppgifterna:

Sverige

Vid överföring till tredje land eller internationell organisation, ange den rättsliga grunden (se avsnitt härom ovan):

Ej aktuellt.