PERSONUPPGIFTSBITRÄDESAVTAL

(PUB-AVTAL)

JML. ART. 28 EUROPAPARLAMENTETS OCH

RÅDETS FÖRORDNING (EU) 2016/679 (GDPR)

Bilaga A till Tjänsteavtal – Journalsystemet Cosmic

mellan

[KOMMUNENS FULLSTÄNDIGA NAMN]

i egenskap av Personuppgiftsansvarig

(nedan ”Personuppgiftsansvarige” eller ”Kommunen”)

och

REGION JÖNKÖPINGS LÄN

i egenskap av Personuppgiftsbiträde

(nedan ”Personuppgiftsbiträdet” eller ”Regionen”)

Avtalsdatum: [DATUM]

Diarienummer Region: [DNUMMER]

Diarienummer Kommun: [DNUMMER]

Version: 1.0

UTKAST

1.0 BAKGRUND

A. Parterna har ingått ett ("Samverkansavtal") avseende samverkan inom hälso- och sjukvård daterat [DATUM] med diarienummer [DNUMMER] ("Samverkansavtalet") samt ett tjänsteavtal avseende kommunal åtkomst till journalsystemet Cosmic daterat [DATUM] ("Tjänsteavtalet").

B. Inom ramen för Tjänsteavtalet behandlar Regionen, i egenskap av ("Systemansvarig") och driftansvarig för Cosmic, ("Personuppgifter") för Kommunens räkning. Den dokumentation som ("Kommunens") ("Användare") registrerar i Cosmic lagras, säkerhetskopieras, driftas och tillgängliggörs av Regionen.

C. Regionen är därmed att betrakta som ("Personuppgiftsbiträde") åt ("Kommunen") avseende den personuppgiftsbehandling som sker för Kommunens räkning, i den mening som avses jml. art. 4.8 och art. 28 ("GDPR").

D. Parternas informationsdelning sker inom ramen för lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation häri benämnd ("SVOD-lagen"), vilken sedan den 1 januari 2023 ersätter de tidigare bestämmelserna om sammanhållen journalföring i 6 kap. ("Patientdatalagen") (2008:355). SVOD-lagen reglerar förutsättningarna för direktåtkomst och annat elektroniskt utlämnande av Personuppgifter mellan vårdgivare och omsorgsgivare.

E. Regionen har genomfört en konsekvensbedömning avseende dataskydd ("DPIA") jml. art. 35 GDPR avseende införande av kommunala användare i Cosmic. De riskreducerande åtgärder som identifierats i DPIA:n utgör en integrerad del av de säkerhetsåtgärder som detta PUB-avtal hänvisar till.

F. Detta avtal utgör Bilaga A till Tjänsteavtalet och syftar till att uppfylla kraven i art. 28.3 GDPR samt säkerställa skydd för de ("Registrerades") rättigheter och friheter vid den ("Behandling") som sker för Kommunens räkning.

G. Parterna noterar att detta PUB-avtal utgör den rättsligt mest utslagsgivande handlingen i avtalsnomenklaturen. Vid motstridighet mellan PUB-avtalets bestämmelser om Dataskydd och Personuppgiftsbehandling och övriga Avtalshandlingar skall PUB-avtalets bestämmelser anses äga fullt företräde.

Mot denna bakgrund har Parterna träffat följande personuppgiftsbiträdesavtal:

2.0 DEFINITIONER

2.1 Utöver de definitioner som anges i Samverkansavtalet och Tjänsteavtalet skall följande termer och uttryck ha den innebörd så som anges jml. GDPR, art. 4. I detta avtal används särskilt:

''Behandling'' avser varje åtgärd eller kombination av åtgärder beträffande personuppgifter, jml. art. 4.2 GDPR.
''Dokumenterade instruktioner'' avser de skriftliga anvisningar som ("Personuppgiftsansvarige") lämnar till Personuppgiftsbiträdet avseende behandlingen, inklusive detta avtal, Bilaga 1 till detta PUB-avtal, Tjänsteavtalet samt eventuella kompletterande skriftliga instruktioner.
''GDPR'' avser 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 (dataskyddsförordningen).
''Patientdatalagen'' eller **''PDL''** avser patientdatalagen (2008:355).
''Personuppgift'' avser varje upplysning som avser en identifierad eller identifierbar fysisk person jml. art. 4.1 GDPR.
''Personuppgiftsansvarig'' avser Kommunen, som bestämmer ändamålen och medlen för den Behandling av Personuppgifter som sker inom ramen för Kommunens hälso- och sjukvårdsverksamhet och som dokumenteras i Cosmic jml. art. 4.7 GDPR.
''Personuppgiftsbiträde'' avser Regionen, som behandlar Personuppgifter för Personuppgiftsansvariges räkning genom att drifta, lagra, säkerhetskopiera och tillgängliggöra Cosmic jml. art. 4.8 GDPR.
''Personuppgiftsincident'' avser en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt röjande av eller obehörig åtkomst till personuppgifter, jml. art. 4.12 GDPR.
''Registrerad'' avser den fysiska person vars Personuppgifter behandlas, dvs. i huvudsak patienter inom Kommunens hälso- och sjukvårdsverksamhet samt, i fråga om logguppgifter, Kommunens Användare.
''SVOD-lagen'' avser lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation.
''Tillsynsmyndighet'' avser Integritetsskyddsmyndigheten (IMY).
''Tredjeland'' avser stat utanför EU/EES-området som inte omfattas av beslut om adekvat skyddsnivå jml. art. 45 GDPR.
''Underbiträde'' avser tredje part som Personuppgiftsbiträdet anlitar för att utföra viss del av Behandlingen för Personuppgiftsansvariges räkning.

3.0 BEHANDLINGENS FÖREMÅL, ART, ÄNDAMÅL OCH VARAKTIGHET

3.1 Föremål

3.1.1 Personuppgiftsbiträdet behandlar Personuppgifter för Personuppgiftsansvariges räkning i samband med drift, lagring, säkerhetskopiering, underhåll och tillgängliggörande av journalsystemet Cosmic, inom vilket Kommunens hälso- och sjukvårdspersonal dokumenterar och tar del av patientinformation.

3.2 Art av behandling

3.2.1 Behandlingen omfattar följande typer av behandlingsåtgärder:

(a) lagring av elektroniska patientjournaler och journalanteckningar;

(b) säkerhetskopiering och återställning av data;

(c) teknisk drift och underhåll av systeminfrastrukturen;

(d) tillgängliggörande av data genom teknisk åtkomst (direktåtkomst) för behöriga Användare;

(e) loggning av all åtkomst till patientdata;

(f) systemuppgraderingar och patchhantering; samt

(g) databasadministration, inklusive indexering och prestandaoptimering.

3.3 Ändamål

3.3.1 Behandlingen sker uteslutande för ändamålet att möjliggöra Kommunens hälso- och sjukvårdsdokumentation och informationsinhämtning jml. ("PDL"), SVOD-lagen och gällande föreskrifter. Personuppgiftsbiträdet får inte behandla personuppgifterna för något annat ändamål.

3.4 Varaktighet

3.4.1 Behandlingen pågår så länge Tjänsteavtalet och Samverkansavtalet är i kraft. Vid Avtalens upphörande regleras hanteringen jml. pkt. 15.0.

4.0 KATEGORIER AV Registrerade OCH PERSONUPPGIFTER

4.1 Kategorier av registrerade

4.1.1 Behandlingen avser Personuppgifter om följande kategorier av registrerade:

UTKAST

(a) patienter som erhåller eller har erhållit hälso- och sjukvård inom Kommunens ansvarsområde (hemsjukvård, särskilt boende, korttidsboende, dagverksamhet, kommunal rehabilitering);

(b) närstående till patienter, i den mån uppgifter om dessa dokumenteras i journalen; samt

(c) Användare (Kommunens personal), vars Personuppgifter förekommer som författare av journalanteckningar och i åtkomstloggar.

4.2 Kategorier av personuppgifter

4.2.1 Behandlingen omfattar följande kategorier av personuppgifter:

Kategori	Exempel	Skyddsnivå
Identitetsuppgifter	Namn, personnummer, folkbokföringsadress, kontaktuppgifter	Hög
Hälsouppgifter (art. 9 GDPR)	Diagnoser, anamnes, bedömningar, vårdplaner, läkemedel, provsvar, funktionsbedömningar	Särskild kategori – mycket hög
Genetiska uppgifter (art. 9 GDPR)	Genetiska analysresultat (i förekommande fall)	Särskild kategori – mycket hög
Biometriska uppgifter	I förekommande fall (t.ex. foto i journal)	Särskild kategori – mycket hög
Uppgifter om sociala förhållanden	Familjesituation, boendeform, närstående	Hög
Administrativa uppgifter	Vårdkontakter, remisser, SIP, samordningsuppgifter	Hög
Logguppgifter	Användaridentitet, tidpunkt, åtkomsttyp, patient-ID	Hög

4.3 Särskilda kategorier av personuppgifter

4.3.1 Parterna konstaterar att Behandlingen i huvudsak avser uppgifter om hälsa jml. art. 9.1 GDPR. Den rättsliga grunden för Behandling av dessa uppgifter utgörs av art. 9.2 (h) GDPR jämte PDL. Behandlingen är nödvändig för tillhandahållande av hälso- och sjukvård och för förvaltning av hälso- och sjukvårdstjänster.

5.0 PERSONUPPGIFTSANSVARIGES SKYLDIGHETER

5.1.1 Personuppgiftsansvarige (Kommunen) ansvarar för:

(a) att Behandlingen sker jml. GDPR, PDL, SVOD-lagen och därmed tillhörande lagstiftning;

(b) att det finns en tillämplig rättslig grund för behandlingen;

(c) att de Registrerade informeras om Behandlingen jml. art. 13 och 14 GDPR;

(d) att lämna ("Dokumenterade") instruktioner till Personuppgiftsbiträdet;

(e) att genomföra och uppdatera konsekvensbedömning (DPIA) i samverkan med Personuppgiftsbiträdet;

(f) att inte instruera Personuppgiftsbiträdet att behandla Personuppgifter på ett sätt som strider mot GDPR eller jml. tillämplig lag;

(g) att genomföra och dokumentera loggkontroller avseende Kommunens Användares åtkomst i Cosmic, jml. 4 kap. 3 § PDL och 4 kap. 4 § SVOD-lagen;

(h) att hantera de registrerades rättigheter jml. pkt. 10.0; samt

(i) att anmäla Personuppgiftsincidenter till Tillsynsmyndigheten jml. pkt. 11.0, i den mån Kommunen finner sig anmälningsskyldig.

6.0 PERSONUPPGIFTSBITRÄDETS SKYLDIGHETER

6.1 Allmänna skyldigheter (art. 28.3 GDPR)

6.1.1 Personuppgiftsbiträdet skall:

(a) behandla personuppgifterna enbart i enlighet med Personuppgiftsansvariges Dokumenterade instruktioner, inklusive vad avser överföring till ("Tredjeland"), och omedelbart underrätta Personuppgiftsansvarige om Biträdet anser att en instruktion strider mot GDPR eller annan unionsrättslig eller nationell dataskyddslagstiftning (art. 28.3 (a) GDPR);

(b) säkerställa att personal som behandlar personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av lagstadgad tystnadsplikt (art. 28.3 (b) GDPR);

(c) vidta alla tekniska och organisatoriska åtgärder som krävs jml. art. 32 GDPR (pkt. 8.0);

(d) inte anlita ("Underbiträde") utan Personuppgiftsansvariges föregående specifika eller allmänna skriftliga godkännande (pkt. 9.0);

(e) bistå Personuppgiftsansvarige vid fullgörandet av dennes skyldighet att hantera de registrerades rättigheter (pkt. 10.0);

UTKAST

(f) bistå Personuppgiftsansvarige vid fullgörandet av skyldigheterna i art. 32–36 GDPR (pkt. 11.0 och 12.0);

(g) efter avslutad Behandling radera eller återlämna personuppgifterna och radera befintliga kopior, om inte lagring krävs jml. lag (pkt. 15.0);

(h) ge Personuppgiftsansvarige tillgång till all information som krävs för att visa att skyldigheterna i art. 28 GDPR fullgörs, samt möjliggöra och bidra till granskningar och inspektioner (pkt.13.0); samt

(i) omedelbart underrätta Personuppgiftsansvarige om Biträdet får en begäran från Registrerad, Tillsynsmyndighet eller annan myndighet som rör de behandlade personuppgifterna.

(j) föra register över de kategorier av Behandling som utförs för Personuppgiftsansvariges räkning jml. art. 30.2 GDPR.

6.2 Behandlingens begränsning

6.2.1 Personuppgiftsbiträdet får inte:

(a) behandla personuppgifterna för egna ändamål;

(b) sammanställa, aggregera eller kombinera Personuppgiftsansvariges Personuppgifter med uppgifter som behandlas för Regionens egen räkning eller för andra personuppgiftsansvarigas räkning, utöver vad som är tekniskt nödvändigt för driften av Cosmic;

(c) överföra personuppgifterna till Tredjeland utan Personuppgiftsansvariges föregående skriftliga godkännande och utan att lämpliga skyddsåtgärder jml. kap. V GDPR har vidtagits; eller

(d) använda personuppgifterna för profilering, automatiserat beslutsfattande, forskning, statistik, AI-träning eller något annat ändamål som inte uttryckligen framgår av Dokumenterade instruktioner.

7.0 SÄRSKILDA BESTÄMMELSER OM SAMMANHÅLLEN VÅRD- OCH OMSORGSDOKUMENTATION

7.1 Rättslig ram

7.1.1 Parternas informationsdelning via Cosmic sker jml. SVOD-lagen, vilken sedan den 1 januari 2023 ersätter de tidigare bestämmelserna om sammanhållen journalföring i 6 kap. PDL. SVOD-lagen reglerar förutsättningarna för direktåtkomst och annat elektroniskt utlämnande mellan vårdgivare och omsorgsgivare.

7.1.2 SVOD-bestämmelserna intas i detta PUB-avtal, och inte enbart i Tjänsteavtalet, eftersom SVOD-lagens krav på direktåtkomst, spärr, samtycke och loggkontroll

utgör behandlingsåtgärder jml. art. 4.2 GDPR vilka skall regleras i det avtal som uppfyller art. 28.3 GDPR.

7.2 Förutsättningar för åtkomst (3 kap. 1 § SVOD-lagen)

7.2.1 Personuppgiftsbiträdet skall säkerställa att de tekniska systemen i Cosmic stödjer de förutsättningar som SVOD-lagen uppställer för att en vårdgivare skall få behandla en annan vårdgivares tillgängliggjorda uppgifter:

(a) att uppgifterna rör en patient som det finns en aktuell patientrelation med;

(b) att patienten samtycker till åtkomsten (om inte undantag föreligger); samt

(c) att uppgifterna kan antas ha betydelse för den vård som patienten behöver.

7.2.2 Personuppgiftsbiträdet ansvarar för att Cosmics tekniska funktionalitet möjliggör registrering och kontroll av samtycke, patientrelation och behov.

7.3 Informationsskyldighet (2 kap. 2 § SVOD-lagen)

7.3.1 Personuppgiftsansvarige (Kommunen) ansvarar för att patienten informeras om vad sammanhållen vård- och omsorgsdokumentation innebär och om möjligheten att motsätta sig att uppgifter görs tillgängliga. Personuppgiftsbiträdet skall tillhandahålla tekniskt stöd i Cosmic för dokumentation av att patienten informerats.

7.4 Spärr (2 kap. 3–5 §§ SVOD-lagen)

7.4.1 Personuppgiftsbiträdet skall säkerställa att Cosmic tekniskt stödjer patientens rätt att spärra uppgifter jml. SVOD-lagen, inklusive:

(a) möjligheten för patienten att motsätta sig att uppgifter görs tillgängliga;

(b) att uppgift om att spärrade uppgifter finns görs tillgänglig för andra vårdgivare utan att röja innehållet;

(c) att uppgift om vilken vårdgivare som spärrat uppgifterna tillgängliggörs under de förutsättningar som anges i 3 kap. 5–6 §§ SVOD-lagen (fara för liv eller allvarlig risk för hälsa); samt

(d) att forcering av spärr loggas särskilt och kan kontrolleras.

7.5 Behörighetsstyrning och loggkontroll (4 kap. SVOD-lagen)

7.5.1 SVOD-lagens krav på behörighetstilldelning och loggkontroll regleras närmare i Tjänsteavtalets pkt. 5.0 och 8.0 samt Bilaga C och H. Personuppgiftsbiträdet ansvarar för att den tekniska plattformen möjliggör efterlevnad av dessa krav, medan Personuppgiftsansvarige ansvarar för att organisatoriskt tillse att behörighetstilldelning, loggkontroll och uppföljning genomförs.

UTKAST

7.6 Vårdgivarens ansvar vid SVOD

7.6.1 Parterna noterar att Kommunen och Regionen är separata vårdgivare jml. 1 kap. 1 § SVOD-lagen. Vardera Part bär därför självständigt ansvaret som vårdgivare för sin egen personuppgiftsbehandling i Cosmic. PUB-avtalet reglerar enbart det biträdesförhållande som uppstår genom att Regionen driftar systemet; det förändrar inte Parternas ställning som självständiga vårdgivare.

8.0 TEKNISKA OCH ORGANISATORISKA SÄKERHETSÅTGÄRDER (ART. 32 GDPR)

8.1 Allmänt

8.1.1 Personuppgiftsbiträdet skall, med beaktande av den senaste tekniken, genomförandekostnaderna, behandlingens art, omfattning, sammanhang och ändamål samt riskerna för de registrerades rättigheter och friheter, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

8.2 Minimiåtgärder

8.2.1 Personuppgiftsbiträdet skall minst vidta följande åtgärder:

8.2.2 Konfidentialitet

(a) stark autentisering med tvåfaktorsautentisering (SITHS-kort eller motsvarande) för all åtkomst till Cosmic;

(b) rollbaserad behörighetsstyrning jml. Tjänsteavtalets pkt. 5.0 och Bilaga D;

(c) krypterad dataöverföring med TLS 1.2 eller senare;

(d) kryptering av lagrade data (encryption at rest) på server- och databasnivå;

(e) nätverkssegmentering som separerar kommunal trafik från Regionens övriga nätverkstrafik;

(f) fysisk åtkomstbegränsning till serverhallar och driftmiljöer; samt

(g) sekretessåtaganden för all personal med tillgång till driftmiljön.

8.2.3 Integritet (riktighet)

(a) transaktionsloggning som möjliggör spårning av alla ändringar i patientdata;

(b) versionering av journalanteckningar (ingen fysisk radering av signerade poster);

(c) checksummekontroll vid säkerhetskopiering; samt

(d) validering av dataintegritet vid återställning.

UTKAST

8.2.4 Tillgänglighet

(a) redundant systemarkitektur (klustrade servrar, redundant lagring);

(b) regelbunden säkerhetskopiering jml. pkt. 8.3;

(c) dokumenterad och testad katastrofåterställningsplan (DRP); samt

(d) servicenivåer jml. bilaga B till Tjänsteavtalet.

8.2.5 Spårbarhet

(a) fullständig loggning av all åtkomst till patientdata (4 kap. 3 § PDL, 4 kap. 4 § SVOD-lagen);

(b) loggar bevaras i minst tio (10) år jml. 3 kap. 17 § PDL;

(c) loggarna skyddas mot manipulation och obehörig åtkomst; samt

(d) logguttag tillhandahålls Personuppgiftsansvarige kvartalsvis och vid begäran.

8.3 Säkerhetskopiering

8.3.1 Personuppgiftsbiträdet skall genomföra säkerhetskopiering av Cosmic-databasen jml. följande:

(a) fullständig säkerhetskopia minst en (1) gång per dygn;

(b) inkrementell säkerhetskopia minst var fjärde (4:e) timme;

(c) lagring av säkerhetskopior på geografiskt separerad plats inom Sverige;

(d) kryptering av säkerhetskopior; samt

(e) regelbunden testning av återställningsförmåga, minst en (1) gång per halvår.

8.4 Kontinuerlig förbättring

8.4.1 Personuppgiftsbiträdet skall årligen se över och vid behov uppdatera de tekniska och organisatoriska säkerhetsåtgärderna med beaktande av den tekniska utvecklingen, nya hotbilder och erfarenheter från incidenter och revisioner.

9.0 UNDERBITRÄDEN

9.1 Godkännande

9.1.1 Personuppgiftsbiträdet får inte anlita Underbiträde för Behandling av Personuppgifter som omfattas av detta avtal utan Personuppgiftsansvariges föregående skriftliga godkännande. Personuppgiftsansvarige lämnar härmed ett allmänt skriftligt godkännande av de Underbiträden som anges i Bilaga 2 till detta PUB-avtal.

9.2 Nya eller ändrade Underbiträden

9.2.1 Personuppgiftsbiträdet skall underrätta Personuppgiftsansvarige skriftligen minst sextio (60) dagar före anlitande av nytt Underbiträde eller byte av befintligt Underbiträde. Underrättelsen skall innehålla:

(a) Underbiträdets identitet, organisationsnummer och säte;

(b) beskrivning av den Behandling som Underbiträdet skall utföra;

(c) var Behandlingen skall äga rum (geografisk lokalisering); samt

(d) vilka säkerhetsåtgärder Underbiträdet vidtar.

9.3 Personuppgiftsansvarige äger rätt att framställa invändning mot anlitande av nytt eller ändrat Underbiträde inom trettio (30) dagar från mottagandet av underrättelsen. I händelse av att den Personuppgiftsansvarige framställer sådan invändning skall Parterna, utan oskäligt dröjsmål och med iakttagande av den lojalitetsplikt som följer av avtalsförhållandet, genom samråd söka nå en ömsesidigt tillfredsställande lösning avseende den fråga som givit upphov till invändningen. Uppnås inte enighet mellan Parterna äger den Personuppgiftsansvarige rätt att säga upp Tjänsteavtalet med en uppsägningstid om tre (3) månader. PUB-avtalet, i den mån det utgör en rättslig förpliktelse, kan inte vara föremål för självständig uppsägning utan följer Tjänsteavtalets bestånd. Uppsägning skall således alltid avse Tjänsteavtalet i första hand, varvid PUB-avtalet upphör att gälla som en följd därav.

9.4 Krav på Underbiträdesavtal

9.4.1 Personuppgiftsbiträdet skall genom skriftligt avtal ålägga varje Underbiträde samma dataskyddsförpliktelser som följer av detta PUB-avtal. Personuppgiftsbiträdet förblir fullt ansvarigt gentemot Personuppgiftsansvarige för Underbiträdets fullgörande av sina skyldigheter.

9.5 Godkända Underbiträden

9.5.1 Förteckning över vid avtalets ingående godkända Underbiträden framgår av Bilaga 2 till detta PUB-avtal.

10.0 BISTÅND VID HANTERING AV REGISTRERADES RÄTTIGHETER

10.1 Allmänt

10.1.1 Personuppgiftsbiträdet skall, med hänsyn till behandlingens art och genom lämpliga tekniska och organisatoriska åtgärder, bistå Personuppgiftsansvarige vid fullgörandet av dennes skyldighet att svara på begäran från Registrerade om utövande av deras rättigheter jml. kap. III GDPR.

UTKAST

10.2 Särskilda rättigheter

10.2.1 Personuppgiftsbiträdet skall särskilt kunna bistå med:

(a) rätt till tillgång (art. 15 GDPR): tillhandahålla kopia av den Registrerades Personuppgifter i Cosmic;

(b) rätt till rättelse (art. 16 GDPR): genomföra teknisk rättelse eller tillägg i Cosmic på instruktion av Personuppgiftsansvarige;

(c) rätt till radering (art. 17 GDPR): i den mån radering inte strider mot journalföringsskyldigheten jml. PDL, utföra radering på instruktion;

(d) rätt till begränsning (art. 18 GDPR): teknisk begränsning av behandling;

(e) rätt till dataportabilitet (art. 20 GDPR): export av den Registrerades uppgifter i strukturerat, maskinläsbart format;

(f) rätt till information om åtkomstlogg (8 kap. 5 § PDL, 4 kap. 5 § SVOD-lagen): tillhandahålla logguttag avseende den Registrerades uppgifter; samt

(g) rätt till spärr (2 kap. 3 § SVOD-lagen, 4 kap. 4 § PDL): tekniskt verkställa och upprätthålla spärrar.

10.3 Tidsfrister

10.3.1 Personuppgiftsbiträdet skall besvara begäran om bistånd från Personuppgiftsansvarige utan onödigt dröjsmål, dock senast inom tio (10) arbetsdagar. Vid komplexa uttag som kräver omfattande tekniskt arbete skall Personuppgiftsbiträdet inom samma tidsfrist meddela uppskattad leveranstid.

11.0 PERSONUPPGIFTSINCIDENTER

11.1 Underrättelseskyldighet

11.1.1 Personuppgiftsbiträdet skall utan onödigt dröjsmål, och under alla omständigheter senast inom tjugofyra (24) timmar efter att ha fått kännedom om en Personuppgiftsincident som berör Personuppgiftsansvariges personuppgifter, underrätta Personuppgiftsansvarige.

11.2 Innehåll i underrättelsen

11.2.1 Underrättelsen skall innehålla minst:

(a) en beskrivning av Personuppgiftsincidentens art, inbegripet, om möjligt, de kategorier av och det ungefärliga antalet Registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs;

(b) namn på och kontaktuppgifter till kontaktpunkt hos Personuppgiftsbiträdet;

UTKAST

(c) en beskrivning av de troliga konsekvenserna av incidenten; samt

(d) en beskrivning av de åtgärder som vidtagits eller föreslås för att åtgärda incidenten och begränsa dess negativa effekter.

11.3 Bistånd vid anmälan

11.3.1 Personuppgiftsbiträdet skall bistå Personuppgiftsansvarige vid:

(a) anmälan av Personuppgiftsincident till Tillsynsmyndigheten (IMY) jml. art. 33 GDPR;

(b) eventuell underrättelse till Registrerade jml. art. 34 GDPR;

(c) anmälan till IVO jml. Patientsäkerhetslagen (2010:659); samt

(d) utredning av incidentens orsak, omfattning och konsekvenser.

11.4 Dokumentation

11.4.1 Personuppgiftsbiträdet skall dokumentera alla Personuppgiftsincidenter, inklusive omständigheter, effekter och vidtagna åtgärder. Dokumentationen skall bevaras i minst fem (5) år och skall på begäran tillhandahållas Personuppgiftsansvarige och Tillsynsmyndigheten.

12.0 KONSEKVENSBEDÖMNING OCH FÖRHANDSSAMRÅD

12.1.1 Personuppgiftsbiträdet skall, med beaktande av behandlingens art och den information som Biträdet förfogar över, bistå Personuppgiftsansvarige vid genomförande och uppdatering av konsekvensbedömningar avseende dataskydd (DPIA) jml. art. 35 GDPR, samt vid eventuellt förhandssamråd med Tillsynsmyndigheten jml. art. 36 GDPR.

12.1.2 Personuppgiftsbiträdet har, i egenskap av vårdgivare och inom ramen för det samarbete som följer av lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation, genomfört en konsekvensbedömning avseende dataskydd jml. art. 35 GDPR, (DPIA), för införandet av kommunala Användare i Cosmic (daterad [DATUM], diarienummer [DNUMMER]). Nämnda konsekvensbedömning avser de risker som är hänförliga till Personuppgiftsbiträdets del av för denne jml. lag krävande egen behandling. Den Personuppgiftsansvarige är oaktat detta skyldig att självständigt genomföra en egen konsekvensbedömning avseende dataskydd som täcker de risker som följer av den Personuppgiftsansvariges Personuppgiftsansvar, inbegripet sådana risker som inte omfattas av Personuppgiftsbiträdets bedömning. De riskreducerande åtgärder som framgår av Personuppgiftsbiträdets konsekvensbedömning och som sammanfattas i Bilaga H till Tjänsteavtalet skall utgöra en integrerad del av detta PUB-avtals säkerhetsåtgärder, utan att detta inskränker den Personuppgiftsansvariges

UTKAST

skyldighet att vidta de ytterligare åtgärder som den egna konsekvensbedömningen föranleder.

13.0 GRANSKNING OCH REVISION (ART. 28.3 (H) GDPR)

13.1 Informationsskyldighet

13.1.1 Personuppgiftsbiträdet skall ge Personuppgiftsansvarige tillgång till all information som krävs för att visa att skyldigheterna i art. 28 GDPR fullgörs.

13.2 Revisionsrätt

13.2.1 Personuppgiftsansvarige har rätt att, själv eller genom en oberoende tredje part som omfattas av tystnadsplikt, genomföra granskningar (revisioner) av Personuppgiftsbiträdets Behandling av Personuppgifter jml. detta avtal. Revisioner skall:

(a) aviseras skriftligen minst trettio (30) dagar i förväg;

(b) genomföras under kontorstid och med hänsyn till Personuppgiftsbiträdets verksamhet;

(c) begränsas till vad som är nödvändigt för att verifiera efterlevnad av detta avtal och GDPR; samt

(d) inte medföra obehörig åtkomst till andra personuppgiftsansvarigas uppgifter.

13.3 Kostnader

13.3.1 Vardera Part bär sina egna kostnader för revision, om inte revisionen påvisar väsentliga brister hos Personuppgiftsbiträdet, i vilket fall Personuppgiftsbiträdet skall bära skäliga kostnader för revisionen.

13.4 Certifieringar och rapporter

13.4.1 I stället för, eller som komplement till, revision kan Personuppgiftsbiträdet tillhandahålla:

(a) certifieringsintyg (t.ex. ISO 27001);

(b) revisionsrapporter från oberoende tredje part (t.ex. SOC 2 Type II); eller

(c) resultatet av penetrationstester genomförda av oberoende säkerhetsföretag.

13.4.2 Sådana intyg eller rapporter befriar inte Personuppgiftsbiträdet från skyldigheten att möjliggöra revision vid begäran.

UTKAST

14.0 ÖVERFÖRING TILL TREDJELAND

14.1.1 Personuppgiftsbiträdet får inte överföra Personuppgifter till Tredjeland eller internationell organisation utan Personuppgiftsansvariges föregående skriftliga godkännande. Vid godkänd överföring skall minst ett av följande villkor vara uppfyllt:

(a) beslut om adekvat skyddsnivå jml. art. 45 GDPR;

(b) lämpliga skyddsåtgärder jml. art. 46 GDPR, inklusive EU-kommissionens standardavtalsklausuler (SCC), bindande företagsbestämmelser (BCR) eller godkänd uppförandekod; eller

(c) undantag jml. art. 49 GDPR, efter dokumenterad bedömning.

14.1.2 Vid avtalets ingående bekräftar Personuppgiftsbiträdet att all Behandling av Personuppgifter jml. detta avtal sker inom Sverige. Eventuell framtida förändring av behandlingsland kräver föregående skriftligt godkännande och, i förekommande fall, uppdatering av DPIA:n.

15.0 UPPHÖRANDE OCH HANTERING AV Personuppgifter VID AVTALETS SLUT

15.1 Personuppgiftsansvariges val

15.1.1 Vid detta PUB-avtals upphörande skall Personuppgiftsansvarige skriftligen instruera Personuppgiftsbiträdet att antingen:

(a) återlämna samtliga Personuppgifter till Personuppgiftsansvarige i ett strukturerat, maskinläsbart format; eller

(b) radera samtliga Personuppgifter och befintliga kopior, inklusive säkerhetskopior.

15.1.2 Personuppgiftsansvarige skall lämna sin instruktion senast trettio (30) dagar före avtalets upphörande. Om instruktion uteblir skall radering ske.

15.2 Undantag – lagstadgad bevarandeskyldighet

15.2.1 Skyldigheten att radera gäller inte i den mån personuppgifterna måste bevaras jml. lag, särskilt:

(a) 3 kap. 17 § PDL, (minst tio år); samt

(b) arkivlagen (1990:782) och kommunens eller regionens arkiveringsreglemente.

15.2.2 Personuppgiftsbiträdet skall i sådant fall säkerställa att uppgifterna skyddas jml. GDPR under hela bevarandetiden och inte behandlas för andra ändamål.

UTKAST

15.3 Övergångsperiod

15.3.1 En övergångsperiod om minst tre (3) månader skall gälla jml. Tjänsteavtalets pkt. 15.4 Under övergångsperioden kvarstår samtliga skyldigheter jml. PUB-avtalet.

15.4 Avvecklingsplan

15.4.1 Parterna skall senast vid den tidpunkt då Personuppgiftsansvarige lämnat instruktioner jml. pkt. 15.1.1 gemensamt upprätta en skriftlig avvecklingsplan. Avvecklingsplanen skall ange:

(a) vilka kategorier av Personuppgifter som skall återlämnas respektive raderas;

(b) vilka kategorier av Personuppgifter som måste bevaras med stöd av lagstadgad bevarandeskyldighet jml. pkt. 15.2. och pkt. 17.1.3.;

(c) den rättsliga grunden för bevarande av varje sådan kategori;

(d) beräknad bevarandetid för respektive kategori;

(e) tidsplan för genomförande av återlämning, radering och migrering; samt

(f) de kategorier av Personuppgifter för vilka personuppgiftsansvaret övergår till Regionen jml. pkt. 15.6.

Avvecklingsplanen skall undertecknas av båda Parter.

15.5 Bekräftelse

15.5.1 Personuppgiftsbiträdet skall efter genomförd radering eller återlämning skriftligen bekräfta till Personuppgiftsansvarige att samtliga Personuppgifter (utöver lagstadgade bevarandekrav) har raderats eller återlämnats, inklusive eventuella kopior hos Underbiträden.

15.6 Övergång av personuppgiftsansvar vid avtalets upphörande

15.6.1 I den mån Personuppgiftsbiträdet efter PUB-avtalets upphörande och efter genomförd återlämning eller radering jml. pkt. 15.1. alltjämt innehar Personuppgifter som Personuppgiftsbiträdet är skyldigt att bevara enligt egen, självständig rättslig förpliktelse – däribland, men inte begränsat till, åtkomstloggar jml. 4 kap. 3 § PDL, dokumentation som krävs jml. arkivlagen (1990:782) för Regionens egen arkivbildning, samt uppgifter som krävs för fullgörande av Regionens skyldigheter jml. Patientsäkerhetslagen (2010:659) – skall Regionen från och med den tidpunkt då biträdesförhållandet upphör anses vara självständigt Personuppgiftsansvarig för dessa kvarvarande personuppgifter.

15.6.2 Personuppgiftsansvaret enligt denna punkt omfattar enbart sådana Personuppgifter som Regionen har en egen rättslig grund att bevara. Det omfattar inte journaldata eller annan patientdokumentation som tillhör Kommunens hälso- och sjukvårdsverksamhet och som skall återlämnas eller raderas jml. pkt. 15.1.1.

UTKAST

15.6.3 Regionen, i egenskap av personuppgiftsansvarig skall jml. nedan:

(a) behandla de kvarvarande personuppgifterna enbart för det ändamål som den lagstadgade bevarandeskyldigheten avser;

(b) vidmakthålla lämpliga tekniska och organisatoriska säkerhetsåtgärder jml. art. 32 GDPR;

(c) uppfylla informationsskyldigheten gentemot Registrerade jml. art. 13 och 14 GDPR, i den mån det är genomförbart och proportionerligt; samt

(d) radera personuppgifterna så snart den rättsliga grunden för bevarande upphör.

15.6.4 Parterna skall i samband med avtalets upphörande gemensamt dokumentera vilka kategorier av Personuppgifter som övergår till Regionens självständiga personuppgiftsansvar, den rättsliga grunden för varje kategori samt den beräknade bevarandetiden. Dokumentationen skall undertecknas av båda Parter och utgöra en del av den avvecklingsplan som upprättas jml. pkt. 15.4 och 17.1.3.

16.0 ANSVAR OCH SKADESTÅND

16.1 Ansvar jml. GDPR

16.1.1 Parternas ansvar mot Registrerade följer av art. 82 GDPR. Vardera Part ansvarar för sin del av en skada som orsakats av Behandling som strider mot GDPR. Personuppgiftsbiträdet ansvarar enbart om det inte har fullgjort de skyldigheter som specifikt åvilar biträden jml. GDPR eller har agerat i strid med eller utanför Personuppgiftsansvariges lagenliga instruktioner.

16.2 Regressrätt

16.2.1 Om en Part har utbetalat full ersättning till en Registrerad jml. art. 82.4 GDPR har den Parten rätt att rikta regresskrav mot den andra Parten för dennes andel av ansvaret.

16.3 Ansvarsbegränsning

16.3.1 Ansvarsbegränsningen i Tjänsteavtalets pkt. 14.3 gäller ej för brott mot detta PUB-avtal. Personuppgiftsbiträdets ansvar under detta PUB-avtal är, för varje skadevållande händelse, begränsat till [BELOPP] kronor, dock inte vid uppsåt, grov vårdslöshet eller brott som medför sanktionsavgift jml. art. 83 GDPR.

16.4 Sanktionsavgifter

16.4.1 Om Tillsynsmyndigheten utfärdar sanktionsavgift (art. 83 GDPR) mot endera Part till följd av Behandling som omfattas av detta avtal, skall den Part vars handling eller underlåtenhet föranledde sanktionsavgiften bära kostnaden. Om

UTKAST

sanktionsavgiften beror på båda Parternas agerande skall kostnaden fördelas i proportion till respektive Parts ansvar.

16.5 Skadeslöshet

16.5.1 Personuppgiftsbiträdet skall hålla Personuppgiftsansvarige skadeslös avseende krav, anspråk och kostnader som riktas mot Personuppgiftsansvarige och som har sin grund i Personuppgiftsbiträdets brott mot detta PUB-avtal, GDPR eller Dokumenterade instruktioner. Omvänt skall Personuppgiftsansvarige hålla Personuppgiftsbiträdet skadeslös avseende krav som har sin grund i Personuppgiftsansvariges instruktioner som strider mot GDPR.

17.0 AVTALSTID OCH SAMBAND MED ÖVRIGA AVTAL

17.1.1 Detta PUB-avtal träder i kraft samma dag som Tjänsteavtalet och gäller så länge Personuppgiftsbiträdet behandlar Personuppgifter för Personuppgiftsansvariges räkning. PUB-avtalet upphör att gälla när samtliga Personuppgifter har raderats eller återlämnats jml. pkt. 15.0, med förbehåll för vad som anges i pkt. 17.1.2. och 17.1.3.

17.1.2 PUB-avtalet kan inte sägas upp separat under löpande Tjänsteavtal. Om Tjänsteavtalet upphör, upphör PUB-avtalet jml. pkt. 15.0, dock med förbehåll för de bestämmelser som enligt sin natur skall bestå efter avtalets upphörande, däribland bestämmelserna om konfidentialitet pkt. 6.1.1 (b), ansvar och skadestånd pkt. 16.0. samt radering och återlämning (pkt. 15.0).

17.1.3 PUB-avtalets upphörande befriar inte Part från skyldigheter som följer av tvingande lag. Vardera Part kvarstår, oaktat PUB-avtalets upphörande, som ansvarig för fullgörande av sina skyldigheter, i synnerhet:

(a) 3 kap. 17–18 §§ Patientdatalagen (2008:355), avseende skyldigheten att bevara journalhandlingar i minst tio år efter det att den sista uppgiften fördes in samt att iaktta arkivlagens krav för journalhandlingar som utgör allmänna handlingar;

(b) 3–6 §§ arkivlagen (1990:782), avseende skyldigheten att bevara, ordna och vårda myndighetens arkiv, inbegripet det förbud mot gallring som följer av kommunens eller regionens arkiveringsreglemente;

(c) 25 kap. offentlighets- och sekretesslagen (2009:400), avseende sekretess för uppgifter om enskildas hälsotillstånd och andra personliga förhållanden inom hälso- och sjukvården;

(d) art. 17.3 (b) och (c) GDPR, avseende undantag från rätten till radering när Behandlingen är nödvändig för fullgörande av rättslig förpliktelse eller för arkivändamål av allmänt intresse;

(e) Patientsäkerhetslagen (2010:659), jml. skyldigheter knutna till patientsäkerhet, händelseanalys och rapportering som kan förutsätta fortsatt tillgång till dokumentation; samt

(f) SVOD-lagen, i den mån Behandling av Personuppgifter fortfarande sker med stöd av SVOD-lagen under den övergångsperiod som avses jml. pkt. 15.3.

17.1.4 I den mån Personuppgiftsbiträdet efter PUB-avtalets upphörande alltjämt behandlar Personuppgifter med stöd av lagstadgad bevarandeskyldighet jml. pkt. 17.1.3, skall Personuppgiftsbiträdet säkerställa att sådana Personuppgifter skyddas jml. GDPR under hela bevarandetiden, att Behandlingen begränsas till det ändamål som den lagstadgade skyldigheten avser, samt att de tekniska och organisatoriska säkerhetsåtgärder som vid PUB-avtalets upphörande tillämpades på personuppgifterna vidmakthålls i skälig utsträckning.

17.1.5 Den uppräkning av lagstiftning som görs i pkt. 17.1.3. är inte uttömmande. Vardera Part ansvarar självständigt för att identifiera och efterleva vid var tid gällande lagstiftning som ålägger Parten skyldigheter avseende bevarande, sekretess eller annan Behandling av Personuppgifter efter PUB-avtalets upphörande.

18.0 AVTALSHIERARKI OCH FÖRETRÄDE

18.1.1 Vid motstridighet mellan handlingar avseende frågor om dataskydd och personuppgiftsbehandling skall, med förbehåll för vad som följer av vid var tid gällande tvingande lagstiftning, följande prioritetsordning gälla mellan avtalshandlingarna:

(a) detta PUB-avtal (inklusive bilagor);

(b) Tjänsteavtalet;

(c) Samverkansavtalet; samt

(d) övriga bilagor i nummerordning.

18.1.2 PUB-avtalet utgör den rättsligt mest kritiska handlingen i den samlade avtalsregleringen. Inga bestämmelser i Samverkansavtalet eller Tjänsteavtalet skall tolkas som inskränkningar av Personuppgiftsansvariges rättigheter eller Personuppgiftsbiträdets skyldigheter jml. detta PUB-avtal.

19.0 ÄNDRINGAR

19.1.1 Ändringar av och tillägg till detta PUB-avtal skall vara skriftliga och undertecknade av behöriga företrädare för båda Parterna. Om GDPR, PDL, SVOD-lagen eller annan tillämplig dataskyddslagstiftning ändras på ett sätt som väsentligen påverkar detta avtals innehåll, skall Parterna utan onödigt dröjsmål anpassa avtalet.

UTKAST

20.0 TVISTLÖSNING OCH TILLÄMPLIG LAG

20.1.1 Tvister i anledning av detta PUB-avtal skall i första hand lösas genom förhandling mellan Parterna. Om förhandling inte leder till uppgörelse inom trettio (30) dagar skall tvisten avgöras av allmän domstol med [ORT] tingsrätt som första instans. Svensk lag skall tillämpas.

20.1.2 Parterna noterar att en Registrerad har rätt att vända sig direkt till Tillsynsmyndigheten eller till domstol jml. art. 77–79 GDPR, oberoende av detta avtals tvistlösningsbestämmelse.

21.0 UNDERSKRIFTER

21.1.1 Detta PUB-avtal har upprättats i två (2) likalydande exemplar, varav Parterna tagit var sitt.

FÖR PERSONUPPGIFTSANSVARIGE (Kommunen):	FÖR PERSONUPPGIFTSBITRÄDET (Regionen):
_____	_____
Namn:	Namn:
Titel:	Titel:
Datum:	Datum:

UTKAST

BILAGA 1 TILL PUB-AVTALET – INSTRUKTIONER FÖR BEHANDLINGEN

Denna bilaga utgör Personuppgiftsansvariges Dokumenterade instruktioner till Personuppgiftsbiträdet jml. art. 28.3 (a) GDPR och 6.1.1 (a) i PUB-avtalet.

1. Instruktion om behandlingens art och ändamål

Personuppgiftsbiträdet instrueras att behandla Personuppgifter enbart genom drift, lagring, säkerhetskopiering, underhåll och tillgängliggörande av journalsystemet Cosmic för Personuppgiftsansvariges hälso- och sjukvårdsverksamhet.

2. Instruktion om säkerhet

Personuppgiftsbiträdet skall vidta de säkerhetsåtgärder som anges i PUB-avtalets pkt. 8, Tjänsteavtalets pkt. 9.0 och Bilaga F och G till Tjänsteavtalet, samt de riskreducerande åtgärder som framgår av DPIA:n (Bilaga H till Tjänsteavtalet).

3. Instruktion om loggning

Personuppgiftsbiträdet skall logga all åtkomst till patientdata jml. 4 kap. 3 § PDL och 4 kap. 4 § SVOD-lagen. Loggar skall bevaras i minst tio (10) år och tillhandahållas Personuppgiftsansvarige kvartalsvis och vid begäran.

4. Instruktion om Tredjelandsöverföring

Personuppgiftsbiträdet skall inte överföra Personuppgifter utanför Sverige utan föregående skriftliga godkännande.

5. Instruktion om bistånd

Personuppgiftsbiträdet skall bistå Personuppgiftsansvarige vid registrerades rättigheter, personuppgiftsincidenter, DPIA och revision jml. PUB-avtalets pkt. 10–13. Vidare skall Personuppgiftsbiträdet bistå i all väsentlig lagupprätthållande verksamhet så som loggkontroll, utelämnande av loggar och handläggning i de fall pkt. 10.0–13.0 tillämpas.

6. Instruktion vid upphörande

Vid PUB-avtals upphörande skall Personuppgiftsbiträdet återlämna eller radera personuppgifterna jml. pkt. 15.0 och den instruktion som Personuppgiftsansvarige lämnar vid den tidpunkten.

Skyldigheten att radera gäller dock inte i den mån personuppgifterna måste bevaras enligt tvingande lag. Personuppgiftsbiträdet är skyldigt att bevara sådana Personuppgifter som omfattas av lagstadgad bevarandeskyldighet enligt de lagrum som anges i pkt. 17.1.3. i PUB-avtalet, däribland:

UTKAST

(a) 3 kap. 17–18 §§ patientdatalagen (2008:355), avseende skyldigheten att bevara journalhandlingar i minst tio år samt att iaktta arkivlagens krav för journalhandlingar som utgör allmänna handlingar;

(b) 3–6 §§ arkivlagen (1990:782), avseende skyldigheten att bevara, ordna och vårda myndighetens arkiv; samt

(c) 25 kap. offentlighets- och sekretesslagen (2009:400), avseende fortsatt sekretess för uppgifter om enskildas hälsotillstånd.

Under den tid Personuppgifter bevaras med stöd av ovan angivna lagrum skall Personuppgiftsbiträdet säkerställa att uppgifterna skyddas jml. GDPR, att Behandlingen begränsas till det ändamål som den lagstadgade skyldigheten avser, samt att de tekniska och organisatoriska säkerhetsåtgärder som tillämpades vid PUB-avtalets upphörande vidmakthålls i skälig utsträckning, jml. pkt. 17.1.4. i PUB-avtalet.

För det fall Personuppgiftsbiträdet efter genomförd återlämning eller radering alltjämt innehar Personuppgifter med stöd av egen rättslig förpliktelse, övergår personuppgiftsansvaret för dessa uppgifter till Regionen jml. pkt. 15.6. i PUB-avtalet.

Den uppräkning av lagstiftning som görs ovan och i pkt. 17.1.3. är inte uttömmande. Vardera Part ansvarar självständigt för att identifiera och efterleva vid var tid gällande lagstiftning som ålägger Parten skyldigheter avseende bevarande, sekretess eller annan Behandling av Personuppgifter efter PUB-avtalets upphörande.

UTKAST

BILAGA 2 TILL PUB-AVTALET – GODKÄNDA UNDERBITRÄDEN

Följande Underbiträden är vid avtalets ingående godkända av Personuppgiftsansvarige:

Underbiträde	Org. nummer	Behandling	Behandlingsland
Cambio Healthcare Systems AB	[ORG.NR]	Systemleverantör; licens, underhåll och uppgraderingar av Cosmic	Sverige
[Ytterligare Underbiträde]	[ORG.NR]	[Beskrivning av driftuppdraget]	Sverige
[Ytterligare Underbiträde]	[ORG.NR]	[Beskrivning]	[Land]

Personuppgiftsansvarige har rätt att begära att Personuppgiftsbiträdet tillhandahåller kopia av relevanta delar av Underbiträdesavtal för granskning, med förbehåll för kommersiell sekretess.

UTKAST

BILAGA 3 TILL PUB-AVTALET – KONTAKTUPPGIFTER

Personuppgiftsansvarige (Kommunen)

Kontaktperson dataskydd: [Namn, titel, e-post, telefon]

Dataskyddsombud (DSO): [Namn, e-post, telefon]

IT-säkerhetsansvarig: [Namn, e-post, telefon]

Incidentrapportering: [E-post och jourlinje]

Personuppgiftsbiträdet (Regionen)

Kontaktperson dataskydd: [Namn, titel, e-post, telefon]

Dataskyddsombud (DSO): [Namn, e-post, telefon]

IT-säkerhetschef: [Namn, e-post, telefon]

Cosmic-Systemförvaltare: [Namn, e-post, telefon]

Incidentrapportering: [E-post och jourlinje]

UTKAST

Motivering till val av egenutformat personuppgiftsbiträdesavtal

Ingår ej i avtalet utan skall utgöra kompletterande noteringar

SKR-mallens tillämpningsområde och begränsningar

Adda/SKR-mallen är utformad som en generisk standardmall avsedd att täcka ett brett spektrum av biträdesförhållanden inom kommunal och regional sektor. Mallen uppfyller de formella minimikraven i art. 28.3 GDPR och utgör en god utgångspunkt för enklare behandlingar. Den har emellertid utformats utan hänsyn till de särskilda förutsättningar som gäller vid Behandling av hälsodata i journalsystem, sammanhållen vård- och omsorgsdokumentation eller den komplexa partsrelation som uppstår när en kommun och en region delar journalsystem.

De mest framträdande begränsningarna i standardmallen, sett i relation till den aktuella behandlingen, kan sammanfattas enligt följande:

Avsaknad av SVOD-reglering. Mallen innehåller inga bestämmelser om sammanhållen vård- och omsorgsdokumentation. Cosmic möjliggör direktåtkomst mellan vårdgivare, vilket regleras av SVOD-lagen. Utan avtalsreglering av spärr, forcering, behörighetsstyrning och loggkontroll saknas den rättsliga ramen för denna centrala funktionalitet.

Generiska säkerhetskrav. Mallen föreskriver "lämpliga tekniska och organisatoriska åtgärder" utan att specificera vilka. För Behandling av hälsodata i ett journalsystem krävs konkreta, verifierbara krav – exempelvis kryptering, tvåfaktorsautentisering och nätverkssegmentering – för att uppfylla det proportionalitetskrav som art. 32 GDPR uppställer.

Avsaknad av DPIA-bestämmelser. Mallen reglerar inte konsekvensbedömning avseende dataskydd (DPIA). Behandlingen i Cosmic utgör högriskbehandling jml. art. 35 GDPR, vilket förutsätter att DPIA genomförs och att dess riskreducerande åtgärder integreras i avtalsstrukturen.

Otillräcklig reglering vid avtalets upphörande. Mallens bestämmelser om upphörande föreskriver radering eller återlämning, men saknar reglering av den situation som uppstår när lagstadgad bevarandeskyldighet (exempelvis 3 kap. 17–18 §§ patientdatalagen eller arkivlagen) förhindrar radering. Utan explicit ansvarsövergång och avvecklingsplan riskerar Personuppgifter att hamna i ett rättsligt vakuum.

Kort underbiträdestid. Mallen föreskriver 30 dagars förvarning vid byte av underbiträde. Vid Behandling av hälsodata i ett journalsystem, där ett byte av underbiträde kan medföra väsentliga säkerhetsrisker, bedöms 60 dagar vara nödvändigt för att möjliggöra en fullständig riskbedömning.

Övriga noteringar och motiveringar:

1. SVOD-AVSNITTET I PUB-AVTALET — VICTORIAS FRÅGA

SVOD-avsnittet (pkt. 7.0) bör ligga under PUB-avtalet av följande motivering:

SVOD-lagen reglerar *personuppgiftsbehandling* — direktåtkomst över vårdgivargränser är en Behandling jml. art. 4.2 GDPR. PUB-avtalet är det avtal som jml. art. 28.3 GDPR reglerar *all* Behandling som biträdet utför. Om SVOD-bestämmelserna flyttas ut ur PUB-avtalet uppstår eventuellt en lucka: biträdet behandlar Personuppgifter (tillgängliggör data mellan vårdgivare) utan att det regleras i PUB-avtalet.

Tjänsteavtalet reglerar SVOD:s *operativa* sida (pkt. 4.0 — informationsskyldighet, samtycke, spärrprocess). PUB-avtalet reglerar SVOD:s *dataskyddsrättsliga* sida (tekniska krav på spärr, loggning, behörighet). D.v.s. ingen dubbelreglering, utan komplementär reglering.

Förslag: SVOD behålls i PUB-avtalet. Tillagd motiveringsmening i pkt. 7.1 (Rättslig ram):

SVOD-bestämmelserna intas i detta PUB-avtal, och inte enbart i Tjänsteavtalet, eftersom SVOD-lagens krav på direktåtkomst, spärr, samtycke och loggkontroll utgör behandlingsåtgärder jml. art. 4.2 GDPR vilka skall regleras i det avtal som uppfyller art. 28.3 GDPR.

UTKAST