Region Jönköpings län

Utfärdare/Enhet	Telefon	Datum	Version	Sida 1 (10)
Projekt	Noteringar			Informationsklass

Avtalskonstruktion för kommunal åtkomst till Cosmic

Utgör ej utkast jmf. avtalen utan skall intolkas som bakgrundsinformation och göra parterna mer införstådda med avtalsmängden.

Innehållsförteckning

1 Inledning 3
2 Struktur på Avtalskonstruktionen 3
3 Hierarki och inbördes företräde 6
4 Avtalsmallens utformning 7
5 Varför ett egenutformat PUB-avtal? 7
6 Rättslig grund 8
7 Frågor för fortsatt övervägande 8
8 Platshållare 9
9 Rekommenderad beslutsordning 9
10 Vanliga frågor 10

1 Inledning

1.1 Detta dokument beskriver den avtalskonstruktion som tagits fram för att reglera kommunernas åtkomst till Region Jönköpings läns journalsystem Cosmic. Informationen häri utgör beslutsunderlag för tjänstemän, förtroendevalda och juridiska granskare.

1.2 Hänvisningar i detta dokument till “vi”, “oss” eller “vår” är till Region Jönköpings Län. Referenser till ”tjänster” avser såväl rådgivning som andra tjänster och inkluderar dokument och andra arbetsresultat.

1.3 Samtliga avtal föreligger i utkastform, det vill säga ingen handling är undertecknad och ingen förpliktelse har uppstått. Syftet med att presentera utkasten är att möjliggöra ett principiellt ställningstagande till avtalsverkets konstruktion och principiella innehåll, innan Parterna slutförhandlar de praktiska detaljerna. Belopp, tidsfrister, servicenivåer, behörighetskonfigurationer och övriga operativa parametrar skall fastställas gemensamt inför undertecknande.

1.4 Detta dokument behandlar avtalens inbördes förhållande, den rättsliga grunden för dess utformning, skälen till att ett egenutformat personuppgiftsbiträdesavtal har valts framför en standardmall, hur avtalsmallarna är uppställda samt vilka frågor som alltjämt kan kvarstå för fortsatt övervägande och vad som återstår att färdigställa inför undertecknande.

2 Struktur på Avtalskonstruktionen

2.1 Avtalsverket består av tre sammankopplade avtal som gemensamt reglerar samtliga aspekter av kommunernas nyttjande av Cosmic. Strukturen är hierarkisk: ett övergripande samverkansavtal fastställer den strategiska ramen, under detta ett tjänsteavtal som reglerar de operativa villkoren, och därunder ett personuppgiftsbiträdesavtal som reglerar dataskyddet.

2.2 Strukturen är avsedd att tillhandahålla Parterna en utökad möjlighet till löpande samarbetsformer avseende informationsdelning och IT-tjänster. Detta innebär att ytterligare tjänsteavtal kan upprättas för de mjukvaror, databaser eller tjänster som Parterna finner lämpligt att inbegripa i samarbetet. Som exempel på en ytterligare tjänst som lämpar sig att reglera inom ramen för en liknande avtalsstruktur kan nämnas nyttjandet av den digitala tjänsten Visiba Care, vilken utgör en applikation inom vilken bland annat Personuppgifter hanteras mellan Parterna.

2.3 Samverkansavtalet

2.3.1 Samverkansavtalet utgör den övergripande juridiska och administrativa ramen för Parternas samarbete inom hälso- och sjukvård. Avtalet bygger vidare på det befintliga KomHem-avtalet (reviderat den 14 juni 2018) vilket reglerar det kommunala övertagandet av hemsjukvård jml. 12 kap. 4 § hälso- och

sjukvårdslagen (2017:30). Samverkansavtalet ersätter inte KomHem-avtalet utan kompletterar detta med en struktur för digital samverkan och informationsdelning.

2.3.2 Avtalet reglerar:

a) **Styrning och organisation**. En gemensam styrgrupp med företrädare för Parterna skall övervaka samverkan, godkänna tjänsteavtal samt följa upp fastställda mål och kvalitetsindikatorer.

b) **Livscykelhantering av tjänster**. Avtalet fastställer hur nya digitala tjänster initieras, ändras och avvecklas. Varje tjänst regleras i ett eget tjänsteavtal vilka utgör bilaga till Samverkansavtalet.

c) **Personuppgiftsbehandling och sekretess**. Övergripande principer för Personuppgiftsansvar, sekretess i enlighet med offentlighets- och sekretesslagen (2009:400) samt informationssäkerhet.

d) **Finansiering**. Vardera Part bär sina egna kostnader såvida inte annat avtalas i tjänsteavtal.

e) **Avtalstid och upphörande**. Avtalet gäller tillsvidare med möjlighet till årlig uppsägning. Vid upphörande skall pågående tjänsteavtal avvecklas i enlighet med respektive tjänsteavtals bestämmelser, varvid Parterna skall tillse att patientvården säkerställs under avvecklingsperioden.

2.4 Tjänsteavtalet

2.5 Tjänsteavtalet utgör Bilaga 4 till Samverkansavtalet och reglerar de operativa, tekniska och verksamhetsmässiga villkoren för kommunens nyttjande av Cosmic. Avtalet utgår från att kommunen nyttjar Cosmic som sitt primära journalsystem för HSL samt att Regionen agerar i egenskap av systemägare, licensinnehavare och driftansvarig.

2.6 Avtalet innehåller följande huvuddelar:

a) **Parternas roller och ansvarsfördelning**. Avsnittet klargör tre centrala scenarier: (i) kommunen dokumenterar i Cosmic i egenskap av eget HSL-system, varvid Regionen agerar som Personuppgiftsbiträde, (ii) samverkan över vårdgivargränser genom sammanhållen vård- och omsorgsdokumentation, varvid vardera Part är självständigt Personuppgiftsansvarig, samt (iii)

samarbetets upphörande, varvid PUB-avtalets bestämmelser om avveckling och ansvarsövergång aktualiseras.

b) **Behörighetsstyrning och åtkomstkontroll**. Detaljerade krav på hur behörigheter tilldelas, ändras och avregistreras. Tilldelningen bygger på principen om minimibehörighet och vårdrelation i enlighet med 4 kap. 1 § patientdatalagen (2008:355). Periodisk behörighetsöversyn skall genomföras var sjätte månad.

c) **Patientdatalagens särskilda skyldigheter**. Inre sekretess, patientens rätt till spärr i enlighet med 4 kap. 4 § PDL, rätt till information och logguttag samt dokumentationsskyldighet.

d) **Sammanhållen vård- och omsorgsdokumentation**. Operativa krav avseende informationsskyldighet, samtycke, spärrhantering och loggkontroll i enlighet med SVOD-lagen.

e) **Utbildning och kompetens**. Obligatorisk grundutbildning före tilldelning av behörighet, årlig fortbildning samt dokumenterade utbildningsregister.

f**) Loggkontroll och uppföljning**. Kommunens skyldighet att regelbundet genomföra loggkontroller i enlighet med 4 kap. 3 § PDL, Regionens rätt till kontroll samt åtgärder vid obehörig åtkomst.

g) **Informationssäkerhet**. Övergripande krav, tekniska säkerhetsåtgärder för kommunens klientmiljö, incidenthantering samt säkerhetsrevision.

h) **Servicenivåer (SLA**). Tillgänglighet, support, rapportering och nödförfarande vid driftstopp. Närmare detaljer specificeras i Bilaga B.

i) **Kostnader**. Tjänsten tillhandahålls utan ersättning. Kommunen bär sina egna interna kostnader för hårdvara, nätverksanpassning, personal och utbildning.

j) **Leverantörsberoende och systemförändringar**. Regionen skall underrätta kommunen om väsentliga förändringar i förhållandet till systemleverantören Cambio Healthcare Systems.

k) **Upphörande och övergångsperiod.** Bestämmelserna säkerställer att pågående patientvård inte äventyras, att data exporteras i strukturerat format samt att PUB-avtalets avvecklingsplan efterlevs.

2.7 PUB-avtalet

2.7.1 Personuppgiftsbiträdesavtalet (PUB-avtalet) utgör Bilaga A till Tjänsteavtalet och reglerar den Behandling av Personuppgifter som sker när Regionen driftar Cosmic för kommunens räkning. Avtalet uppfyller samtliga obligatoriska krav som följer av artikel 28.3 i förordning (EU) 2016/679.

2.7.2 PUB-avtalet innehåller följande huvuddelar:

a) **Behandlingens art, ändamål och varaktighet**. Preciserar vad som behandlas, i vilket syfte samt under vilken tidsperiod Behandlingen skall pågå.

b) **Kategorier av registrerade och Personuppgifter**. Omfattar hälsodata i enlighet med artikel 9 i förordning (EU) 2016/679, patientidentitet, vårdrelationer samt logguppgifter.

c) **Särskilda bestämmelser om SVOD-lagen**. Reglerar den dataskyddsrättsliga sidan av sammanhållen vård- och omsorgsdokumentation, inbegripet tekniska krav avseende spärr, forcering, behörighetsstyrning och loggkontroll.

d) **Tekniska och organisatoriska säkerhetsåtgärder**. Specificerade krav avseende bland annat TLS 1.2 eller senare, kryptering vid vila (AES-256), tvåfaktorsautentisering, nätverkssegmentering, säkerhetskopiering (daglig fullständig samt inkrementell var fjärde timme) och tio års loggbevarande.

e) **Underbiträden**. Godkännande, sextio (60) dagars förvarning vid byte samt krav på underbiträdesavtal.

f) **Personuppgiftsincidenter**. Tjugofyra (24) timmars underrättelsefrist, bistånd vid anmälan i enlighet med artikel 33 i förordning (EU) 2016/679 samt dokumentationsskyldighet.

g) **Konsekvensbedömning (DPIA)**. Eget avsnitt med tröskelvärde för omprövning.

3 Hierarki och inbördes företräde

3.1 Avtalen är avsiktligt strukturerade i en hierarki som säkerställer att dataskyddsreglering alltid har företräde. Konstruktionen är väsentlig: utan den skulle bestämmelser i ett överordnat avtal kunna urgräva de dataskyddskrav som GDPR kräver att ett PUB-avtal innehåller.

Nivå	Avtal	Företräde
1 (överst)	Samverkansavtalet	Övergripande ramverk; KomHem-avtalet gäller för grundläggande ansvarsfördelning
2	Tjänsteavtalet (Bilaga 4)	Operativa villkor; underordnat Samverkansavtalet
3	PUB-avtalet (Bilaga A till Tjänsteavtalet)	Äger företräde i samtliga frågor om personuppgiftsbehandling och dataskydd

3.2 PUB-avtalets företräde framgår av samtliga tre avtals hierarkibestämmelser. Konstruktionen säkerställer att dataskyddet inte kan avtalas bort genom motstridiga bestämmelser i de överordnade avtalen.

4 Avtalsmallens utformning

4.1 Avtalen är uppställda i en partsneutral form som inte följer någon enskild Parts grafiska profil. Valet är medvetet och motiveras av tre skäl.

4.2 För det första är avtalen avsedda att gälla mellan Regionen och var och en av länets tretton kommuner. En neutral uppställning signalerar att handlingarna är gemensamt framförhandlade och inte ensidigt formulerade av någondera Part.

4.3 För det andra följer uppställningen den dispositionsmodell som är vedertagen för komplexa avtal i europeisk och svensk avtalspraxis: parternas identifikation, bakgrundsrecitals som etablerar avtalets kontext, ett fristående definitionsavsnitt, materiella bestämmelser ordnade efter sakområde, avslutande bestämmelser (avtalstid, uppsägning, tvist, ändringar) samt underskrifter. Bakgrundsrecitals, stundom benämnda portalbestämmelser, utgör en inledande och vägledande del av avtalet som anger hur kontraktet skall tolkas och som kan innehålla en beskrivning av sammanhanget, syftet eller vad som föregått avtalet. Dispositionsmodellen är den som genomgående tillämpas av ledande nordiska advokatbyråer vid utformning av avtal av motsvarande komplexitet. Valet av en etablerad och igenkännbar struktur underlättar juridisk granskning, förkortar inläsningstiden samt minskar risken för tolkningstvister.

4.4 För det tredje möjliggör den neutrala formen att avtalen kan anpassas till varje enskild kommun utan att layouten behöver göras om.

5 Varför ett egenutformat PUB-avtal?

5.1 Vi har valt att inte tillämpa den standardmall för personuppgiftsbiträdesavtal som tillhandahålls av Adda i samarbete med Sveriges Kommuner och Regioner (SKR) och Inera, version 2.1 daterad den 6 april 2023. Standardmallen är generiskt utformad för ett brett spektrum av biträdesförhållanden. Den uppfyller minimikraven i artikel 28.3 i förordning (EU) 2016/679 men är inte anpassad för den Behandling som här är aktuell.

5.2 De mest framträdande begränsningarna i standardmallen är avsaknad av SVOD-reglering, generiska säkerhetskrav utan specificerade åtgärder, avsaknad av DPIA-bestämmelser, otillräcklig reglering vid avtalets upphörande avseende avvecklingsplan och ansvarsövergång, samt en förvarningsfrist om trettio (30) dagar vid byte av Underbiträde jämfört med sextio (60) dagar i det egenutformade avtalet.

5.3 Det egenutformade avtalet tilläggsreglerar samtliga dessa områden. En fullständig jämförelse framgår av nedanstående tabell.

Område	Egenutformat avtal	SKR-mallen	Motivering
SVOD-lagen	Helt avsnitt (pkt. 7.0)	Saknas	Cosmic hanterar SVOD
AI och profilering	Explicit förbud (pkt. 6.2 d)	Saknas	Art. 22 GDPR
Tekniska säkerhetsåtgärder	TLS 1.2+, AES-256, 2FA	Generiskt	Art. 32 GDPR
Säkerhetskopiering	Daglig full, 4h inkrementell	Saknas	RTO/RPO för journaldata
DPIA	Eget avsnitt (pkt. 12.0)	Saknas	Art. 35 GDPR
Incidentfrist	24 timmar	Utan onödigt dröjsmål	72h-anmälan möjliggörs
Underbiträden	60 dagars förvarning	30 dagar	Riskbedömning av nytt biträde
Avvecklingsplan	Strukturerad (pkt. 15.4)	Saknas	Kritiskt för hälsodata

Ansvarsövergång	Explicit (pkt. 15.6)	Saknas	Förhindrar rättsligt vakuum
Avtalshierarki	PUB äger företräde	Huvudavtalet över PUB	Dataskydd kan ej avtalas bort
Bevarandeskyldighet	Konkreta lagrum (pkt. 17.1.3)	Tvingande lag utan specifikation	Rättssäkerhet
Loggbevarande	10 år	5 år	PDL 3:17

5.4 Förordning (EU) 2016/679 uppställer inga krav på att en viss standardmall skall tillämpas. Artikel 28.3 anger de obligatoriska avtalsvillkoren men överlämnar åt parterna att utforma avtalet efter Behandlingens specifika förutsättningar. Skäl 81 i förordningens ingress understryker att avtalet bör beakta de specifika uppgifter och skyldigheter som Personuppgiftsbiträdet har inom ramen för den Behandling som skall utföras.

5.5 Varför återfinns SVOD-bestämmelserna i PUB-avtalet?

5.5.1 1 SVOD-lagens krav avseende direktåtkomst, spärr, samtycke och loggkontroll utgör behandlingsåtgärder i den mening som avses i artikel 4.2 i förordning (EU) 2016/679. Eftersom artikel 28.3 i samma förordning kräver att all Behandling som Personuppgiftsbiträdet utför skall regleras i PUB-avtalet, är det rättsligt nödvändigt att SVOD-bestämmelserna intas däri. Tjänsteavtalet reglerar SVOD:s operativa sida; PUB-avtalet reglerar den dataskyddsrättsliga sidan. Uppdelningen är komplementär.

6 Rättslig grund

6.1 **EU-nivå**: 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 (allmän dataskyddsförordning), särskilt artikel 28 (Personuppgiftsbiträde), artikel 32 (säkerhet för Behandlingen), artikel 35 (konsekvensbedömning avseende dataskydd) samt artikel 9 (Behandling av särskilda kategorier av Personuppgifter).

6.2 **Nationell nivå**: patientdatalagen (2008:355), lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation (SVOD-lagen), patientsäkerhetslagen (2010:659), offentlighets- och sekretesslagen (2009:400), arkivlagen (1990:782), hälso- och sjukvårdslagen (2017:30), lagen (2017:612) om samverkan vid utskrivning från sluten hälso- och sjukvård samt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

6.3 **Avtalsmässig grund**: KomHem-avtalet (reviderat den 14 juni 2018) samt Samverkansavtalet.

7 Frågor för fortsatt övervägande

7.1 Avtalsverket är genomarbetat, men det finns områden där Parterna kan ha anledning att fördjupa sin gemensamma hållning. Nedanstående punkter utgör inte brister utan frågor som förtjänar juridisk dialog.

7.2 Ansvarsbegränsningens nivå

7.2.1 Såväl PUB-avtalet som Tjänsteavtalet innehåller platshållare för beloppstak. Parterna behöver enas om en nivå som är proportionerlig i förhållande till Behandlingens art och risk. En för lågt satt nivå kan vid tvist anses oskälig; en för högt satt nivå kan vara kommersiellt orimlig. Undantag för uppsåt, grov vårdslöshet och administrativa sanktionsavgifter jml. art. 83 i (EU) 2016/679 är redan reglerade.

7.3 Gemensamt Personuppgiftsansvar

7.3.1 Avtalsverket utgår från att vardera Part är självständigt Personuppgiftsansvarig och att den omständigheten att Parterna nyttjar samma system inte i sig etablerar gemensamt ansvar jml. art. 26 (EU)

2016/679. Bedömningen är förenlig med Integritetsskyddsmyndighetens praxis men kan behöva omprövas om den faktiska Behandlingen förändras.

7.4 KomHem-avtalets giltighet

7.4.1 Samverkansavtalet bygger på KomHem-avtalet, vilket gällde till och med den 31 december 2024 med automatisk förlängning om fem år. Parterna bör säkerställa att förlängningen har skett samt att KomHem-avtalets villkor alltjämt är ändamålsenliga.

7.5 Konsekvensbedömning (DPIA)

7.5.1 Avtalen hänvisar till en konsekvensbedömning avseende dataskydd i enlighet med artikel 35 i förordning (EU) 2016/679 som ännu inte är slutförd. Dess slutsatser kan föranleda justeringar av de säkerhetsåtgärder som specificeras i PUB-avtalet.

7.6 Systemleverantörens roll

7.6.1 Regionen är beroende av Cambio Healthcare Systems i egenskap av systemleverantör. Tjänsteavtalet innehåller en bestämmelse avseende leverantörsberoende, men Parterna bör överväga huruvida ytterligare skyddsmekanismer erfordras.

7.7 Framtida lagstiftning

7.7.1 NIS 2-direktivet (EU) 2022/2555 är under implementering i svensk rätt och kan medföra tillkommande krav avseende informationssäkerhet. Avtalen innehåller en generell klausul om att Parterna skall efterleva vid var tid gällande lagstiftning, men specifika ändringar kan behöva förhandlas.

8 Platshållare

8.1 Avtalstexterna innehåller platshållare som skall fastställas gemensamt: avtalsdatum, diarienummer, kommunens fullständiga namn, belopp för ansvarsbegränsning, behörig tingsrätts säte, antal styrgruppsledamöter, SLA-procent, avtalsperiod samt kontaktpersoner.

8.2 Bilagor

8.2.1 Följande bilagor återstår att upprätta: Bilaga B till Tjänsteavtalet (servicenivåer), Bilaga C (standardkonfiguration), Bilaga D (behörighetsprofiler), Bilaga E (dokumentationsriktlinjer), Bilaga F

8.2.2 (informationssäkerhetspolicy), Bilaga G (tekniska krav på kommunens klientmiljö), Bilaga H (DPIA-utdrag), PUB-avtalets Bilaga 2 (godkända underbiträden) samt Samverkansavtalets Bilaga 1, 3 och 5.

8.2.3 Avtalen innehåller en klausul som medger att bilagor färdigställs successivt under pågående implementeringsprojekt, under förutsättning att de bilagor som är nödvändiga för drift har undertecknats vid driftsättning.

8.3 DPIA

8.3.1 Konsekvensbedömningen skall genomföras eller färdigställas innan avtalen undertecknas.

9 Rekommenderad beslutsordning

a) Parterna fattar principbeslut om att anta avtalsverkets struktur och innehåll.

b) Resurser tillsätts för att färdigställa bilagor, genomföra konsekvensbedömning avseende dataskydd samt fastställa platshållare.

c) Juristerna vars uppdrag varit att utföra den juridiska analysen granskar de slutliga utkasten efter Parternas eventuella tillägg och ändringar.

d) Avtalen undertecknas av behöriga företrädare.

10 Vanliga frågor

10.1 **Är avtalen bindande**? Nej. Samtliga avtal föreligger i utkastform. Bindande verkan uppstår först vid undertecknande av behöriga företrädare.

10.2 **Är Regionen Personuppgiftsbiträde**? Ja. Regionen bestämmer inte ändamålen med kommunens patientdokumentation utan tillhandahåller den tekniska plattformen och behandlar Personuppgifter för kommunens räkning i enlighet med artikel 4.8 och artikel 28 i förordning (EU) 2016/679.

10.3 **Innebär ett delat system gemensamt Personuppgiftsansvar**? Inte per automatik. Vardera Part är självständigt ansvarig. Om en specifik Behandling innebär att Parterna gemensamt bestämmer ändamål och medel kan artikel 26 i förordning (EU) 2016/679 aktualiseras, men detta förutsätter en konkret bedömning i det enskilda fallet.

10.4 **Vad sker med data vid upphörande**? Kommunen väljer mellan återlämning eller radering. En avvecklingsplan upprättas. Data som Regionen har lagstadgad skyldighet att bevara övergår till Regionens Personuppgiftsansvar.

10.5 **Är tjänsten förenad med kostnad**? Nej. Kommunen bär sina egna interna kostnader.

10.6 **Varför har SKR:s standardmall inte tillämpats**? Standardmallen saknar SVOD-reglering, specificerade säkerhetsåtgärder, bestämmelser avseende konsekvensbedömning, avvecklingsplan samt ansvarsövergång. Det egenutformade avtalet är anpassat för hälsodata i ett delat journalsystem.