# Sveus policy för hantering av personuppgifter

## Bilaga 2 - Utökad juridisk beskrivning av hantering av personuppgifter inom Sveus uppföljningssystem

## Dokumenthistorik

| Version | Författare | Beskrivning | Datum godkännande expertgrupp | Datum godkännande styrgrupp |
|---|---|---|---|---|
| 1 | Wohlin, Manolis | Beskrivning av hantering av personuppgifter genom forskningsuttag | Expertgrupp inte formerad | 2014-01-31 |
| 2 | Wohlin, Manolis | Uppdatering och tillägg drift | 2015-04-27 | 2015-04-28 |
| 3 | Manolis, Magné | Uppdatering övergång till förvaltning och GDPR översyn | 2018-12-06 | 2018-12-21 |

# 1 Bakgrund och inledning

Sju landsting och regioner (sjukvårdshuvudmänen) bedrev mellan 2013-2017 ett gemensamt nationellt samverkansprojekt med syftet att utveckla diagnosspecifika värdebaserade uppföljningssystem (”**Sveus**”). Målet var att ge sjukvårdshuvudmän och andra vårdgivare bättre möjligheter att följa upp utförd vård med fokus på effektivitetsutveckling, dvs. förbättrat hälsoutfall och minimerad resursåtgång. Utveckling av ersättningssystem var initialt en del i projektet, men nedprioriterades snart och utvecklingen fokuserade på analys och uppföljning.

Sveus projektet övergick vid årsskiftet 2017/2018 i förvaltning. Genom det samverkansavtal som tecknats mellan deltagande landsting och SKL placerades uppdraget att ansvara för den tekniska förvaltningen av Sveus Analysplattform (förvaltningsobjektet) hos Registercentrum Västra Götaland (RC VGR) inom Västra Götalands läns landsting (VGR).

Ett Nyttjanderättsavtal avseende Sveus Analysplattform har tecknats mellan VGR och Ivbar, undertecknat den 11 juli 2018 med diarienummer RS 2018-03924. För stöd till RC VGR i den tekniska förvaltningen har det även tecknats ett Drift-, underhåll- och supportavtal mellan VGR och Ivbar undertecknat den 11 juli 2018 med diarienummer RS 2018-03923 inklusive bilagor därtill vilka utgörs av Kontaktuppgifter (Bilaga 1), Specifikation (Bilaga 2), Prisbilaga (Bilaga 3), Principer för API (bilaga 4), RS-riktlinjer för Informationssäkerhet i Västra Götalandsregionen (Bilaga 5), ERA: Free and Open Source (FOSS) dependencies (Bilaga 6) och Personuppgiftbiträdesavtal (Bilaga 7).

Detta dokument beskriver hur sekretess och personuppgifter hanteras inom Sveus med utgångspunkt från gällande lagar. Vid tecknande av avtal kan Parter med fördel hänvisa till detta dokument. Dokumentet är uppdelat efter de syften för vilka personuppgifter behandlas. Dokumentet avslutas med ett kort avsnitt om den förändring av rättsläge som lagförslaget i en statlig utredning, SOU2014:23, skulle kunna medföra.

# 2 Allmänt

## 2.1 Klargörande av personuppgiftansvar

Innan personuppgifter behandlas inom ramen för Sveus åligger det den part som ska behandla uppgifterna att ha säkerställt vem som är personuppgiftsansvarig för behandlingen och att de krav som följer av dataskyddsförordningen och annan tillämplig lagstiftning uppfyllts. Med personuppgiftsansvarig avses enligt dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Vem som är personuppgiftsansvarig kan också framgå av författning. Så har skett i patientdatalagen (PDL). Enligt PDL är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför.

Den som är personuppgiftsansvarig för en viss behandling av personuppgifter kan komma att anlita en aktör utanför organisationen för att på dennes vägnar behandla personuppgifter. Denna aktör benämns personuppgiftsbiträde. Enligt dataskyddsförordningen avses med personuppgiftsbiträde en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Mellan personuppgiftsansvarig och personuppgiftsbiträde ska finnas ett skriftligt avtal eller annan rättsakt enligt unionsrätten eller medlemsländernas nationella rätt som reglerar parternas skyldigheter och rättigheter avseende dataskydd.

I Sveus Analysplattform agerar RC VGR genom VGR som personuppgiftsbiträde och primär teknisk förvaltare åt de nämnder hos respektive landsting och region som är anslutna till Sveus. Ivbar är ett

godkänt underbiträde åt RC VGR och bearbetar tekniskt data åt respektive vårdgivare. Ivbar i sin tur anlitar med personuppgiftsansvariges godkännande ett under-underbiträde för teknisk lagring av data inom Sveus.

Som vägledning för aktörerna ska vad som anges i detta dokument tillämpas, om inte annat skriftligen överenskommes mellan Parter.

## 2.2 Informationssäkerhet vid personuppgiftsbehandling

Den som är personuppgiftsansvarig för behandling av personuppgifter som föranleds av Sveus ska tillse att behandlingen är förenlig med dataskyddsförordningens bestämmelser om bl.a. skydd för personuppgifter (se art. 32). Därutöver tillkommer säkerhetskrav i PDL och i Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.

En av nyheterna i dataskyddsförordningen är att personuppgiftsbiträden och underbiträden får ett visst självständigt ansvar för behandlingen av personuppgifter för någon annans räkning. De omfattas numera, liksom personuppgiftsansvariga, av Datainspektionens tillsyn. Den som inom ramen för behandling av personuppgifter som föranleds av Sveus är personuppgiftsbiträde ska se till att behandlingen sker i enlighet med bestämmelserna om personuppgiftsbiträden i dataskyddsförordningen och utfärdade instruktioner från den personuppgiftsansvarige samt att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de personuppgifter som behandlas.

## 2.3 Personuppgifter och aggregering

En grundläggande skillnad föreligger mellan å ena sidan uppgifter som direkt eller indirekt kan knytas till en viss person, s.k. personuppgifter, och å andra sidan sådana uppgifter som inte kan knytas till viss person. För uppgifter som inte kan knytas direkt eller indirekt till en individ gäller varken dataskyddsförordningen, PDL eller sekretess till skydd för enskild.

När uppgifter från flera personer aggregeras så upphör i regel möjligheten att knyta uppgifterna till en person, men integritetsrisker kan ändå föreligga. Man brukar här tala om *röjanderisk*. En sådan situation kan aktualiseras i statistikverksamhet. Problem med röjanderisk uppstår när t.ex. celler i en tabell endast består av ett fåtal uppgiftslämnare. Då kan man inte utesluta att uppgifterna tillsammans kan användas för att indirekt spåra enskilda individer. En personuppgiftsansvarig ska därför applicera metoder för *röjandekontroll* vid offentliggörande av rapporter från källor som innehåller personuppgifter så att uppgifter inte indirekt går att hänföra till en person.

## 2.4 Sekretessavtal

I 2 kap. 1 § offentlighets- och sekretesslagen (OSL) finns det generella förbudet i offentlig förvaltning mot att röja eller utnyttja en uppgift enligt OSL (eller annan författning som OSL hänvisar till). Av bestämmelsen framgår också vilka personer, knutna till en myndighet, som ska följa reglerna om sekretess och tystnadsplikt. Till att börja med har alla anställda hos en myndighet en skyldighet att iaktta sekretess och tystnadsplikt. Även en fysisk person som på grund av uppdrag, t.ex. en konsult, eller ”på annan liknande grund” deltar i myndighetens verksamhet kan omfattas av samma tystnadsplikt som myndighetens anställda.

För att en extern konsult ska omfattas av personkretsen i 2 kap. 1 § OSL krävs att denne är en s.k. osjälvständig uppdragstagare. En osjälvständig uppdragstagare är en fysisk person som har ett

personligt uppdrag hos en myndighet och som har en sådan anknytning till myndigheten att han eller hon kan sägas delta i dennas verksamhet. Med en myndighets verksamhet avses den egentliga verksamheten, den som framgår eller kan utläsas av myndighetens instruktion, reglemente eller av annan författning. En sådan uppdragstagare har den behövliga anknytningen till en viss myndighet, om den uppgift som han eller hon utför vanligen ska fullgöras av en tjänsteman eller någon annan befattningshavare vid myndigheten eller i varje fall naturligen skulle kunna handhas av en sådan befattningshavare. Typiskt för osjälvständiga uppdragstagare är att myndigheten har tecknat ett uppdragsavtal med uppdragstagaren (och inte ett företag), att uppdragstagaren är underkastad myndighetens arbetsledning eller uppdragstagaren bedriver sitt arbete i myndighetens lokaler.

OSL gäller emellertid i princip inte för den som är anställd hos ett företag som i sin tur har ett uppdragsavtal med en myndighet. Externa konsulter som anlitas av Regionstyrelsen i Västra Götalands län, via ett företag som Regionstyrelsen har avtal med, faller därmed utanför OSL:s bestämmelser. Undantagsvis kan dock en extern konsult lyda under OSL:s bestämmelser, nämligen om denne ställs till myndighetens förfogande och deltar i dess verksamhet på samma sätt som om myndigheten hade ingått uppdragsavtal med vederbörande själv.[1] Med avseende på sådana situationer omfattas även den som ”på annan liknande grund” deltar i myndighets verksamhet av personkretsen. I sådana och liknande fall gäller 2 kap. 1 § OSL:s röjandeförbud även den som på ”annan liknande grund” deltar i myndighets verksamhet. Så är dock som regel inte fallet för utomstående experter som rådfrågas av Regionstyrelsen utan att något egentligt uppdragsavtal föreligger.

Externa konsulter som anlitas av Regionstyrelsen genom avtal med företaget (inte med konsulten) omfattas således också av tystnadsplikten i 2 kap. 1 § OSL om denne ställts till Regionstyrelsens förfogande och deltar i Sveus på samma sätt som om Regionstyrelsen hade ingått uppdragsavtal med konsulten själv. En sådan konsult ska erinras om sin tystnadsplikt, liksom konsulter med vilka regionstyrelsen har personliga uppdragsavtal med (se ovan).

Ett personuppgiftsbiträde och dess medarbetare, t.ex. Ivbar, kan däremot inte anses ”delta i myndighetens verksamhet” på det sätt som avses i 2 kap. 1 § OSL eftersom en sådan aktör alltid är någon utanför den personuppgiftsansvariges organisation. Behovet av tystnadsplikt för sådana personer som medverkar i Sveus kan dock tillgodoses genom lagstiftning vid sidan av sekretesslagen.

I situationer då externa konsulter som anlitas som underleverantörer för insatser inom Sveus inte omfattas av någon lagreglerad tystnadsplikt och det heller inte är möjligt att lämna ut uppgifterna med ett sekretessförbehåll enligt OSL, får behovet av tystnadsplikt tillgodoses i rent civilrättslig ordning genom ett personligt avtal om tystnadsplikt, även benämnt sekretessavtal.[2] Den situationen föreligger med avseende på Ivbars medarbetare och medarbetare hos Ivbars underleverantör, givet att medarbetarna enbart behöver ta del av pseudonymiserade uppgifter och personuppgiftsbiträdesavtalet noggrant reglerar förutsättningarna för dessa att ta del av personuppgifter i klartext i undantagsfall.

Genom ingående av avtal med Ivbar under Nyttjanderättsavtalet och Drift-, underhåll- och supportavtalet, och genom användande av individuella sekretessavtal, blir bestämmelserna om ”tystnadsplikt” i avtalen tillämpliga för Ivbar i förhållande till den part som ingått avtal med Ivbar, dvs. tystnadsplikt rörande sådan parts verksamhet och uppdraget inom Sveus.

---

[1] Prop. 1979/80:2 Del A s. 128.

[2] Prop. 1979/80:2 Del A s. 128

Mellan myndigheter involverade i Sveus gäller OSL (dvs. även utan att sekretessåtagande i avtal finns mellan sådana parter).

# 3 Kvalitets- och utvecklingsarbete

Ivbar, som är underbiträde åt personuppgiftsbiträdet VGR, kan inom ramen för Sveus, komma att involveras av vårdgivare för kvalitets- och utvecklingsarbete som innefattar analys av personuppgifter.

För sådan verksamhet inom Sveus har följande varit utgångspunkt för personuppgiftsansvaret:

- Vårdgivaren är personuppgiftsansvarig för aktuellt dataunderlag. Anlitade konsulter tillåts alltså inte bestämma ändamålen och medlen för den behandling som de utför.

I dessa fall ska behandling av personuppgifter ske enligt instruktion från vårdgivarna ifråga. Dataskyddsförordningen stipulerar att ett avtal eller annan rättsakt enligt unionsrätten eller medlemsländernas nationella rätt ska träffas mellan personuppgiftsansvarig och personuppgiftsbiträde vid behandling av personuppgifter. Sådana personuppgiftsbiträdesavtal ska således tecknas mellan varje ansluten vårdgivare och RC VGR genom VGR. Personuppgiftsbiträdesavtalen ska innehålla dokumenterade instruktioner från vårdgivarna till RC VGR. Därutöver ska RC VGR genom VGR teckna ett personuppgiftsbiträdesavtal med Ivbar, som agerar i rollen som s.k. underbiträde. Anlitar Ivbar i sin tur underleverantörer ska bolaget likaså teckna ett personuppgiftsbiträdesavtal med dessa aktörer. Mall för sådant avtal tillhandahålls av RC VGR.

# 4 Drift av uppföljningssystem

Sveus Analysplattform är ett verktyg för sjukvårdshuvudmän och andra vårdgivare som syftar till att förbättra möjligheterna att följa upp och utvärdera den offentligt finansierade hälso- och sjukvården. Den grundläggande idén är att samla och bearbeta data från olika källor, framförallt från vårdgivare och kvalitetsregister, samt via ett webbaserat gränssnitt förmedla underlag för jämförelser och analys som ska underlätta utvecklings- och förbättringsarbete på såväl klinik- och vårdgivarnivå som på beställarnivå.

Sveus uppföljningssystem kan användas vid de deltagande vårdgivarna var för sig. I systemen behandlas känsliga personuppgifter vilket ställer särskilda krav på personuppgiftshantering. Denna personuppgiftshantering beskrivs i detta kapitel 4.

## 4.1 Översikt av juridisk situation vid drift

Sveus uppföljningssystem innefattar personuppgifter från vårdgivare (främst vårdadministrativa databaser) och från kvalitetsregister. Respektive vårdgivare är personuppgiftsansvarig för sin användning av systemen.

RC VGR ansvarar för den tekniska förvaltningen av Sveus uppföljningssystem och analysplattform och är personuppgiftsbiträde för anslutna vårdgivare. På uppdrag av VGR genomför Ivbar, som underbiträde, viss bearbetning av personuppgifterna. Varje vårdgivare erhåller en egen logisk instans av uppföljningssystemet, vilket innebär att personuppgifter inte sambearbetas mellan vårdgivarna. Den tekniska bearbetningen för systematisk uppföljning och kvalitetssäkring samt ersättningshantering är tillåten enligt PDL inom respektive vårdgivares verksamhet. Uppgifterna är när de bearbetas pseudonymiserade i syfte att uppfylla dataskyddsförordningens krav på uppgiftsminimering och kompensera för eventuella integritetsrisker.

## 4.2 Personuppgiftsbehandling vid drift

För användande av uppföljningssystem har följande varit utgångspunkt för personuppgiftsansvar:

- Respektive vårdgivare är personuppgiftsansvarig för sin användning av Sveus uppföljningssystem

### 4.2.1 Lagstöd för databehandling under PDL

*Detta avsnitt beskriver sjukvårdshuvudmannens och andra vårdgivares rätt enligt gällande lag att bearbeta personuppgifter från vårdgivare och kvalitetsregister för systematisk uppföljning och kvalitetssäkring, exempelvis genom Sveus uppföljningssystem.*

En vårdgivare får med stöd av PDL behandla känsliga personuppgifter för ett antal i lagen närmre angivna ändamål, utan att behöva inhämta patientens samtycke. Detta innefattar även ändamål som inte är direkt kopplade till vården av enskilda patienter, inklusive systematisk uppföljning och kvalitetssäkring (2 kap 4 § punkt 4 PDL).

Nationella och regionala kvalitetsregister regleras av 7 kap. PDL. Ett kvalitetsregister är en samling av personuppgifter som ska användas för att analysera och utvärdera hälso- och sjukvård eller tandvård. Personuppgifter i kvalitetsregister ska behandlas för ändamålet att systematiskt och fortlöpande utveckla och säkra vårdens kvalitet (7 kap. 4 §). Dessa personuppgifter får också användas för de sekundära ändamålen (i) framställning av statistik, (ii) forskning inom hälso- och sjukvården och också för (iii) fullgörande av någon uppgiftsskyldighet som följer av lag eller förordning, annan än den som anges i 6 kap. 5 § OSL. Enligt PDL kan dessutom behandling ske för ändamålet utlämnande till den som behöver använda uppgifterna för det primära och de sekundära ändamålen statistik och forskning (dvs. (i)-ii) ovan).

Sjukvårdshuvudmannen får således med stöd av PDL använda patientdata från vård bedriven i egen regi och data som den i egen regi bedrivna vården har lämnat till kvalitetsregister för att systematiskt och fortlöpande utveckla liksom för att säkra kvaliteten i verksamheten och statistik. På de premisser som beskrivs i detta dokument är personuppgiftsbehandlingen i Sveus uppföljningssystem således en tillåten behandling av personuppgifter.

### 4.2.2 Behandling av personuppgifter genom biträde, i drift

*Detta avsnitt beskriver hur Sveus uppföljningssystem kan administreras av en gemensam central organisation för samtliga vårdgivare genom personuppgiftsbiträdesrelation. Varje vårdgivare erhåller en egen logisk instans av uppföljningssystemet, vilket innebär att personuppgifter ej sambearbetas mellan vårdgivare men att aggregerade data kan användas för jämförelse mellan vårdgivare.*

Utifrån förutsättningarna att (i) respektive vårdgivare är personuppgiftsansvarig för sitt uppföljningssystem, (ii) VGR eller annan organisation agerar personuppgiftsbiträde respektive underbiträde åt flera olika vårdgivare samtidigt, (iii) VGR eller annan organisation har dokumenterade instruktioner för att utföra de analyser av patientuppgifter i varje vårdgivares logiska instans av Sveus uppföljningssystem som uppdraget omfattar och (iv) ett personuppgiftsbiträdesavtal finns med varje vårdgivare, kan en koordinerad men ändå klart avgränsad behandling av uppgifter komma till stånd.

Om en personuppgiftsansvarig väljer att behandla personuppgifter med hjälp av ett personuppgiftsbiträde, och överlåter driften till denne, ska personuppgiftsansvarig försäkra sig om att biträdet lever upp till ställda krav i regelverket för dataskydd inklusive informationssäkerhet. Dessa krav tydliggörs i personuppgiftsbiträdesavtalet.

# 4.3 Sekretess vid drift

*Detta avsnitt beskriver begränsningar i nuvarande lagstiftning med avseende på privata vårdgivares och kvalitetsregisters möjlighet att lämna ut patientuppgifter till landsting och regioner (sjukvårdshuvudmännen) samt hur detta skulle kunna avhjälpas för Sveus uppföljningssystem genom att patienten ger sitt skriftliga samtycke. Något sådant utlämnande förekommer inte i dagsläget i Sveus, men övervägs. I avsnittet diskuteras de rättsliga möjligheterna för sjukvårdshuvudmännen att inhämta patientuppgifter från sina privata vårdutförare.*

Sjukvårdshuvudmännen har ett lagstadgat ansvar för den hälso- och sjukvård som med offentliga medel erbjuds och kommer invånarna till godo. För att huvudmännen ska kunna sköta detta ansvar måste det finnas förutsättningar att ta del av och hantera uppgifter som de behöver för att kunna vidta effektiva och ändamålsenliga åtgärder.

I nuläget är sjukvårdshuvudmännens rättsliga möjligheter att få ta del av patientuppgifter hos privata vårdgivare som bedriver hälso- och sjukvård på uppdrag av huvudmännen begränsade då dessa omfattas av tystnadsplikt (enligt patientsäkerhetslag 2010:659, se särskilt 6 kap. 12-16 §§) som omfattar även huvudmännen och andra vårdgivare. De saknar vidare ett tydligt författningsstöd för att behandla andra vårdgivares personuppgifter. Sjukvårdshuvudmännen kan alltså inte nödvändigtvis enkelt leva upp till sitt lagstadgade ansvar att följa upp och kvalitetssäkra de privata vårdgivarnas hälso- och sjukvård. En sjukvårdshuvudman har av samma skäl inte heller rätt att ta del av patientuppgifter i ett kvalitetsregister som en privat vårdgivare har registrerat.

En patient får dock alltid efterge sekretess och tystnadsplikt inom hälso- och sjukvården. Med stöd av patientens samtycke kan en vårdgivare lämna ut patientuppgifter till en mottagare, t.ex. en sjukvårdshuvudman för ändamålet uppföljning, utvärdering och kvalitetssäkring. En patients samtycke att lämna ut hans eller hennes uppgifter är tillåtet under förutsättning att patienten har fått adekvat information om utlämnandet, förstått den och samtyckt. Även en huvudman för ett kvalitetsregister får med stöd av patientens samtycke lämna ut patientuppgifter till en anvisad mottagare, t.ex. en sjukvårdshuvudman. Detta får då ske genom ADB-utlämnande (ej direktåtkomst).

Även om sekretessen är bruten såtillvida att uppgifter lämnats ut från en vårdgivare till en sjukvårdshuvudman kvarstår sekretess som hindrar sjukvårdshuvudmannens möjligheter att lämna ut dessa uppgifter till andra vårdgivare. Om inte denna sekretess efterges kommer vårdgivarnas möjligheter att ta del av patientuppföljning på individnivå över vårdgivargränser att vara kraftigt begränsade.

Samtycke genom vilket patienten efterger sekretessen bör därför omfatta följande utlämnanden och mottagare för att uppgifter ska kunna nyttjas inom Sveus:

1. En privat vårdgivares utlämnande av patientdata till sjukvårdshuvudmannen.
2. Ett kvalitetsregisters utlämnande av patientdata till sjukvårdshuvudmannen.
3. En sjukvårdshuvudmans utlämnande av patientdata till de vårdgivare som har varit involverade i patientens vård och behandling.

Avsnitt 5.1 nedan beskriver de lagförändringar som föreslås i SOU 2014:23. Om dessa genomförs kommer det ovan beskrivna samtycket ej behövas för Sveus uppföljningssystem.

# 5 Övrigt

## 5.1 Möjliga konsekvenser av SOU 2014:23

En statlig utredning (Utredningen om rätt information i vård och omsorg, SOU 2014:23) har föreslagit en tystnadspliktsbrytande uppgiftsskyldighet för privata vårdgivare i förhållande till den sjukvårdshuvudman som har ansvar för att erbjuda den aktuella hälso- och sjukvården. Privata vårdgivare ska lämna ut de personuppgifter som huvudmannen behöver för att planera, följa upp och kvalitetssäkra den hälso- och sjukvård som denne har huvudmannaansvar för. Vidare föreslår utredningen att en vårdgivare förutom att som idag få ha direktåtkomst till de uppgifter om en patient i ett kvalitetsregister som vårdgivaren själv har lämnat utöka tillgången till att även innefatta de uppgifter om patienten som en annan vårdgivare lämnat till samma kvalitetsregister. Förslagen har ännu inte realiserats i lagstiftningen.

Sedermera har Välfärdsutredningen i sitt slutbetänkande Kvalitet i välfärden (SOU 2017:38) också föreslagit bl.a. en uppgiftsskyldighet för privata vårdgivare och privata utförare inom socialtjänsten (avsnitt 10.2.3). Inte heller detta förslag har realiserats.