Per Bergstrand
personuppgiftsombud
per.bergstrand@skane

Personuppgiftbiträdesavtal – en hjälptext

Det här dokumentet är en information och instruktion avseende hantering av BITRÄDESAVTAL vid behandling av PERSONUPPGIFTER.

Dokumentet förklarar vad som menas med *personuppgiftsbiträde*, när s.k. biträdesavtal (eller PUB-avtal) måste ingås, samt vad som menas med *underbiträde* och när avtal även i dessa fall måste ingås. Till dokumentet finns det bilagor med checklistor för att bedöma externa PUB-avtal samt vilka förberedelser en personuppgiftsansvarig bör vidta innan personuppgifter utlämnas till ett biträder.

Sammanfattning:

Så snart någon bestämmer över hanteringen av personuppgifter är denne *personuppgiftsansvarig*. Så snart någon annan hanterar *personuppgifter* för den *personuppgiftsansvariges* räkning så är denne ett *personuppgiftsbiträde*. Ett personuppgiftsbiträde får endast hantera personuppgifter utifrån det uppdrag denne fått från den personuppgiftsansvarige, biträdet får alltså inte ha några egna ändamål för hanteringen.

Så snart någon ska behandla personuppgifter för annans räkning uppstår också ett krav att upprätta ett personuppgiftsbiträdesavtal (biträdesavtal, PUB-avtal, PUBA) som reglerar hur hantering av personuppgifter ska ske mellan parterna. Ett vanligt exempel på när ett personuppgiftsbiträdesavtal krävs är då en IT-leverantör uppdragits att leverera olika typer av IT-tjänster åt en kund, såsom lagringstjänster eller administrativa tjänster vilka involverar personuppgifter. Kunden är då personuppgiftsansvarig, och leverantören blir personuppgiftsbiträde. En förutsättning för att behandling av personuppgifter för en personuppgiftsansvarigs vägnar ska få genomföras av ett biträde är att denne kan ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i Dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. Det kan exempelvis röra sig om garantier avseende personuppgiftsbiträdets kompetens, tillförlitlighet, ekonomiska resurser, rutiner och tillgång till tekniska lösningar.

Om personuppgiftsbiträdet i sin tur anlitar en underleverantör är denne underleverantör ett underbiträde. Även här måste det finnas ett avtal, antingen

direkt med den personuppgiftsansvarige eller att personuppgiftsbiträdet tillåts ingå underbiträdesavtal.

Ett biträdesavtal måste innehålla vissa bestämmelser. Det viktigaste är att beskriva just biträdesförhållandet, dvs. att biträdet inte får hantera personuppgifter för några andra syften eller ändamål än det som beskrivs av tjänsten.

Vem är personuppgiftsansvarig i Region Skåne?

Det är organisationen Region Skåne i sig som är personuppgiftsansvarig, det är alltså inte någon viss person eller funktion. Däremot kan olika funktioner och personer ha ett ansvar för att se till att lagstiftningens krav följs. I Region Skåne pekas den som är informationsägare till en viss informationsmängd ut som den som är ansvarig för att information (inklusive personuppgifter) hanteras i enlighet med interna krav och lagstiftningen. Detta framgår av riktlinjer för informationssäkerhet. (Länk till riktlinjer för informationssäkerhet)

Ansvaret går inte att avtala bort

Region Skåne är ansvarig för all hantering all hantering av personuppgifter som sker i organisationen, även om ett biträde anlitas övergår inte något ansvar. Om ett biträde gör något fel, om personuppgifter röjs, förstörs eller på annat sätt missbrukas är det den personuppgiftsansvarige som står ansvaret. Region Skåne är alltså till exempel ansvarig för vad en ev. kundsupport i gör eller inte gör. Registrerade kan begära skadestånd av Region Skåne direkt om hanteringen strider mot Dataskyddsförordningen, även om det är biträdet som gjort fel. Region Skåne kan sedan förvisso ha en regressrätt mot biträdet.

Vad är ett personuppgiftsbiträde?

Personuppgiftsbiträde definieras som den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Det är alltid den personuppgiftsansvarige som ansvarar för att behandlingen av personuppgifter sker i enlighet med gällande lagstiftning. Detta förändras inte av att personuppgiftsbehandlingen utförs av ett personuppgiftsbiträde. Även personuppgiftsbiträdet har vissa skyldigheter enligt Dataskyddsförordningen (som att vidta nödvändiga tekniska skyddsåtgärder), men *inga* skyldigheter övergår från den ansvarige till biträdet endast för att den personuppgiftsansvarige väljer att anlita ett biträde.

Eftersom ett biträdesförhållande endast uppstår när den ansvarige låter någon annan behandla personuppgifter innebär detta i praktiken att ett personuppgiftsbiträde *måste* vara en extern aktör som inte organisatoriskt hör till den personuppgiftsansvarige.

En grundläggande förutsättning för biträdesförhållandet är att ett personuppgiftsbiträde endast ska utföra behandling av personuppgifterna på

uppdrag av den personuppgiftsansvarige. Det innebär alltså att det måste vara väldigt tydligt uttryckt vilken behandling av personuppgifter som den personuppgiftsansvarige uppdrar åt biträdet att utföra. Normalt sätt framgår detta av det tjänsteavtal som föreligger mellan parterna där en beskrivning av tjänsten som leverantören ska utföra framgår. Förutom detta avtal måste det också finnas ett s.k. biträdesavtal (kallas även personuppgiftsbiträdesavtal, PUB-avtal eller PUBA) som formellt reglerar förhållandet mellan personuppgiftsbiträde och personuppgiftsansvarig avseende just hanteringen av personuppgifter. Finns inget biträdesavtal är detta ett brott mot Dataskyddsförordningen, det är alltså ett *absolut krav* att ett sådant avtal föreligger.

Exempel på biträdessituationer:

En personuppgiftsansvarig har lagt ut del av sin IT-drift på en extern aktör. I praktiken innebär detta att en IT-leverantör hanterar t.ex. lagring och elektronisk kommunikation av data/information. Eftersom informationen innehåller personuppgifter så är IT-leverantören ett personuppgiftsbiträde till den personuppgiftsansvarige.

En personuppgiftsansvarig köper en produkt som innefattar informationshantering. Produkten kan t.ex. vara en medicinteknisk produkt som innefattar hantering av personuppgifter. I många fall levererar leverantören av produkten inte bara den tekniska produkten utan hanterar även den information som produkten samlar in och lagrar. Hanteringen kan innefatta förädling av informationen eller sammanställning eller lagring eller allt detta. Eftersom det inte är den personuppgiftsansvarige som hanterar informationen utan en externa aktör, och detta sker på uppdrag av den personuppgiftsansvarige, är leverantören ett personuppgiftsbiträde till den ansvarige.

En leverantör tillhandahåller utveckling, underhåll och support för ett system som innehåller personuppgifter. Den personuppgiftsansvarige hanterar själv lagring och elektronisk kommunikation av uppgifterna i systemet. Leverantören får åtkomst till personuppgifterna vid support, utvecklings- och underhållsärenden och är därför ett personuppgiftsbiträde som behandlar personuppgifter för den ansvariges räkning. Ett personuppgiftsbiträdesavtal behöver tecknas.

Exempel på vad som INTE är biträdessituationer:

En anställd hos den personuppgiftsansvarige utför en uppgift, t.ex. gör kvalitetsuppföljning som omfattar en stor mängd personuppgifter. Den anställde är inte personuppgiftsansvarig utan endast en medhjälpare till den som är personuppgiftsansvarig (företaget/myndigheten/organisationen som ansvarar för kvalitetsuppföljningen).

En anlitad konsult som arbetar på plats med ett specificerat uppdrag underställd en chef hos den personuppgiftsansvarige. Konsulten är i detta fall att betrakta som en osjälvständig uppdragstagare som arbetar enbart på uppdrag av den personuppgiftsansvarige och lyder under dennes arbetsledning. Konsulten likställs då med en anställd hos den personuppgiftsansvarige och är endast en medhjälpare till denne.

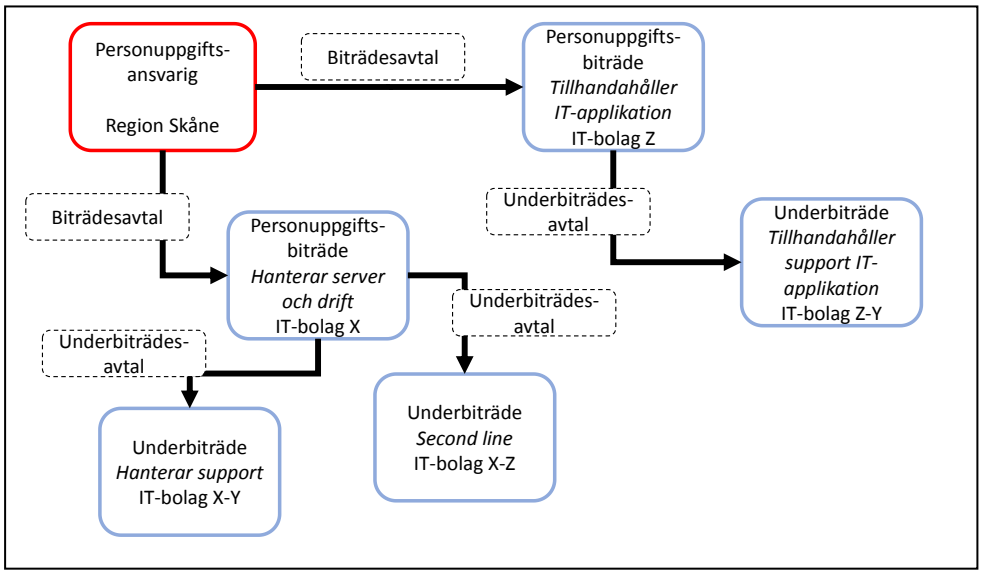
En annan organisation har fått personuppgifter utlämnande från Region Skåne för att bedriva ett eget forskningsprojekt. I detta fall är den andra organisationen personuppgiftsansvariga för den vidare hanteringen av personuppgifter, det är inte Region Skåne som bestämmer över vilka ändamål och medel de kommer att hantera uppgifterna för.

Vad är ett *underbiträde*?

Om den leverantör som behandlar personuppgifter för den personuppgiftsansvariges räkning i sin tur anlitar underleverantörer för att hantera delar av tjänsten så innebär detta att även underleverantören till ett personuppgiftsbiträde är att anses som personuppgiftsbiträden. Underleverantören är att anse som ett personuppgiftsbiträde när de ta emot personuppgifter i den enda avsikten att behandla personuppgifterna för den personuppgiftsansvariges räkning. En sådan underleverantör brukar särskiljas från det första biträdet genom att det första biträdet definieras som *huvudbiträde* och underleverantörer som *underbiträde*.

I de situationer huvudbiträdet anlitar en eller flera underbiträden kan kravet på personuppgiftsbiträdesavtal uppfyllas genom att den personuppgiftsansvarige i biträdesavtalet ger ett huvudbiträde mandat att ingå biträdesavtal med dessa underbiträden. Ger man som personuppgiftsansvarig ett sådant mandat måste det framgå i avtalet att varje underbiträde har samma skyldigheter som huvudbiträdet. Om förutsättningarna för personuppgiftsbehandlingen ser väsentligt annorlunda ut hos ett underbiträde än hos huvudbiträdet kan detta kräva ytterligare villkor för att underbiträdet ska kunna uppnå samma skyldigheter som huvudbiträdet.

En grundläggande förutsättning för att den personuppgiftsansvarige ska kunna uppfylla säkerhetskraven och kravet på kontroll av personuppgiftsbiträden är att den personuppgiftsansvarige har kännedom om vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning. Det ingår alltså i ansvaret som personuppgiftsansvarig att ha kontroll över de som hanterar personuppgifterna och



även skapa sig en uppfattning om att dessa hanterar personuppgifterna på ett säkert sätt.

Vad är ett biträdesavtal (PUB-avtal)?

En grundläggande förutsättning för biträdesförhållandet är att ett personuppgiftsbiträde *endast ska utföra behandling av personuppgifterna på uppdrag* av den personuppgiftsansvarige. Det innebär alltså att det måste vara väldigt tydligt uttryckt vilken behandling av personuppgifter som den personuppgiftsansvarige uppdrar åt biträdet att utföra. Normalt sätt framgår detta av det avtal som föreligger mellan parterna där en beskrivning av tjänsten framgår. Förutom detta måste det finnas ett s.k. biträdesavtal (kallas även personuppgiftsbiträdesavtal, PUB-avtal eller PUBA) som formellt reglerar förhållandet mellan personuppgiftsbiträde och personuppgiftsansvarig.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde måste det alltså finnas ett skriftigt avtal, ett så kallat biträdesavtal. Det är ett ansvar för både den personuppgiftsansvarige och biträdet att ett sådant avtal finns.

Vad ska ett biträdesavtal innehålla?

Lagstiftningen kräver att ett biträdesavtal innehåller vissa delar. Dessa redovisas i bilaga 2. Om leverantörs biträdesavtal används i avtalet måste detta avtal kontrolleras gentemot denna checklista. Om Region Skånes standardavtal används som biträdesavtal behöver inte denna kontroll ske. Däremot ska standardavtalet kompletteras med instruktioner (se nedan).

Vad ett personuppgiftsbiträdesavtal ska innehålla regleras huvudsakligen i artikel 28 i Dataskyddsförordningen. Det måste framgå vilka personuppgifter som är föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, och den personuppgiftsansvariges skyldigheter och rättigheter ska även anges.

Det är viktigt att notera att ett biträdesavtal i mångt och mycket är ett standardavtal som tas fram och som reglerar förhållandet mellan personuppgiftsbiträde och personuppgiftsansvarig. I princip kan det beskrivas som att biträdet garanterar att denne inte vidtar några åtgärder utöver vad som krävs för att utföra tjänsten samt ett antal krav från ansvarig till biträde vad avser säkerhet och garanti för att de registrerades rättigheter respekteras.

För att det ska vara möjligt att utläsa vad biträdet faktiskt får göra med personuppgifterna så *MÅSTE* ett biträdesavtal kombineras med ett tjänsteavtal/huvudavtal där det framgår vad den egentliga tjänsten består av. Utan ett sådant avtal eller alternativt mycket tydliga instruktioner förbjuder ett biträdesavtal i princip all hantering av personuppgifter.

En viktig del av kraven är att biträdet hanterar personuppgifter på ett tillräckligt säkert sätt. Denna skyldighet har biträdet även utifrån Dataskyddsförordningen, det

är alltså även personuppgiftsbiträdets skyldighet att hantera personuppgifter utifrån på ett säkert sätt i förhållande till dess känslighet. En viktig uppgift för den personuppgiftsansvariga är att ge biträdet instruktioner som konkretiserar dessa åtgärder.

Instruktioner till biträdet

Vad gäller dessa konkreta instruktioner ska de vara så tydliga att otillåten behandling inte kommer att utföras. Sådana instruktioner kan exempelvis gälla ändamålet/n med behandlingen, tredjelandsöverföring och under vilka förutsättningar som utlämnande får ske till tredje man. Instruktioner ges lämpligen i en bilaga till biträdesavtalet men kan också framgå av huvudavtalet.

De instruktioner som ges handlar alltså om hur personuppgiftsbitträdet ska hantera personuppgifterna när denne utför sin tjänst. Det handlar således inte om säkerhetskrav på tjänsten i sig.

Exempel: Som konkret exempel så ska ett avtal om ett journalsystem innehålla de krav som ställda på journalsystemet; t.ex. om att det ska finnas möjlighet att hantera spärrar i systemet, att vårdgivarens personal ska loggas i de aktiviteter de gör inom systemet, m.m. Som en del av tjänsten tillhandahåller även leverantören support till systemet, i denna support har leverantören åtkomst till delar av systemet och i denna roll är leverantör personuppgiftsbiträde. I instruktionerna till biträdet skulle då kunna stå att åtkomst endast får ske i anledning av konkret supportärende. Att supportpersonal måste använda sig av stark autentisering vid inloggning m.m. Men det framgår inte här något om de krav som finns på IT-lösningen vad avser patients rätt till spärr etc.

Se exempel på instruktioner till personuppgiftsbiträde i bilaga 3. Observera att även om man använder sig av Region Skåne standardmall för biträdesavtal bör instruktioner som konkretiserar hur biträdet ska hantera säkerheten utformas till biträdet.

Vad gäller kravet på informationssäkerhet måste vidare den personuppgiftsansvarige kunna förvissa sig om att personuppgiftsbiträdet faktiskt *kan* genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna. Det sistnämnda kravet innebär att den personuppgiftsansvarige har ett ansvar att kontrollera att anlitade personuppgiftsbiträden både kan och verkligen vidtar lämpliga säkerhetsåtgärder. Den personuppgiftsansvarige kan alltså *inte enbart* förlita sig på vad som utfästs av biträdet utan måste har gjort en bedömning om denne verkligen kan utföra åtgärderna.

Vad måste den personuppgiftsansvarige tänka på innan ett biträdesförhållande uppstår?

I bilaga 1 finns en mer utförlig checklista för vilka åtgärder som bör vidtas innan personuppgifter utlämnas till ett personuppgiftsbiträde. Innan en tjänst som innebär att ett biträdesförhållande uppstår (t.ex. en molntjänst tas i bruk, eller att personuppgifter lämnas till en extern supportorganisation) måste den

personuppgiftsansvarige bedöma om den behandling av personuppgifter som denne vill låta biträdet (leverantören) utföra kommer att vara tillåten enligt Dataskyddsförordningen och i övrigt följa Regions Skånes riktlinjer för behandling av personuppgifter. Vid denna bedömning måste leverantörens villkor och förmåga att skydda personuppgifterna i tillräckligt hög grad kontrolleras.

Den personuppgiftsansvarige (Region Skåne) måste bland annat:

• ta ställning till om det finns risk för att personuppgifter kan komma att behandlas för andra *ändamål* än de ursprungliga. Det är enbart den personuppgiftsansvarige som förfogar över ändamålen med behandlingen, biträdet ska inte ha möjlighet att hantera personuppgifterna för egna ändamål.

• ta ställning till om biträdet kan komma att lämna över personuppgifter till ett så kallat tredje land, det vill säga ett land utanför EU/EES, och om den överföringen i så fall har stöd enligt Dataskyddsförordningen

• bedöma vilka säkerhetsåtgärder som måste vidtas för att skydda de personuppgifter som behandlas och säkerställa att dessa tillämpas av biträdet. Den ansvarige kan alltså inte förlita sig på vad biträdet erbjuder utan måste själv skapa sig en uppfattning om vilka skydd som krävs och om de uppfylls. Så kan t.ex. ske genom en riskanalys. Det är även ett krav enligt Dataskyddsförordningen att genomföra just en riskanalys (s.k. konsekvensbedömning) om behandlingen av personuppgifterna är integritetsmässigt särskilt känslig.

• se till att ett biträdesavtal upprättas (se checklista nedan över vad ett sådant avtal ska innehålla)

• beakta annan lagstiftning som påverkar hanteringen, till exempel sekretesslagstiftning.

Särskilt om sekretesslagstiftning

Omfattas uppgifterna av Offentlighet- och sekretesslagen (2009:400) (OSL), innebär det att dessa uppgifter är känsliga och omfattas av sekretess. Detta ställer särskilda krav på hur leverantör får hantera uppgifterna.

De närmare kraven ska konkretiseras genom genomförd riskanalys och slås fast i avtal med leverantören, antingen som en del av huvudavtalet, som del av ett personuppgiftsbiträdesavtal eller som ett särskilt sekretessavtal.

Här ska understrykas att denna fråga är komplex och svår att hantera. En särskild problematik när det gäller OSL är att uppgifterna inte otillåtet får *röjas*. Redan genom att uppgifterna överlämnas till en leverantör kan innebära att uppgifterna anses vara röjda, något som är förbjudet enligt lag. För att motverka att uppgifterna ska anses vara röjda kan åtgärder vidtas som gör det mer eller mindre sannolikt att

leverantören faktiskt tar del av uppgifterna. För den som vill läsa mer om rättsläget hänvisas till rapporten ”molntjänster i staten” som pensionsmyndigheten tog fram 2016. http://www.samradsgruppen.se/web/index.php/8-nyheter/151-molntjanster-ny-rapport

I denna rapport framgår: ”Är informationen sekretessreglerad ska myndigheten pröva om det är förenligt med offentlighets- och sekretesslagen att lämna ut informationen till den aktuella molntjänstleverantören eller om sekretess utgör hinder för ett utlämnande. Vid sekretessprövningen måste myndigheten uppmärksamma att prövningen inte enbart ska göras i förhållande till moln-tjänsteleverantören utan också i förhållande till eventuella underleverantörer som an-litas av molntjänstleverantören och som kommer att hantera myndighetens information.”

Det den ansvarige myndigheten ska pröva är huruvida myndigheten har en så pass stor kontroll över hanteringen av uppgifterna att man kan säga sig vara säker på att uppgiften inte röjs för utomstående. Prövningen blir svårare att göra desto högre sekretess det gäller eftersom myndigheten då måste vara ännu säkrare att uppgiften hanteras korrekt (icke-röjd). Som exempel så innebär sjukvårdssekretess ett omvänt skaderekvisit, dvs. för att kunna lämna ut uppgifter måste man vara säker på att den skyddsvärde inte drabbas av men, detta är en mycket hög form av sekretess.

Exempel på åtgärder för att göra det troligt att uppgifter som omfattas av sekretess inte röjs vid utlämnande till personuppgiftsbiträde:

• Åtkomst får bara ske efter tillåtelse från Region Skåne som i så fall ska föregås av en sekretessprövning (är detta möjligt, finns beredskap utanför kontorstid).

• Handläggare som faktiskt tar del av uppgifterna knyts till Region Skåne som osjälvständig uppdragstagare. Typiskt sett en konsult som arbetar i Region Skånes lokaler på uppdrag av Region Skåne och som lyder under lokal chef.

• Uppgifterna får bara hanteras (vara åtkomlig för leverantör eller underleverantör) inom Sveriges rikes gränser.

• Leverantör ska vara certifierad enligt ISO 27001 eller annan likvärdig standard för de delar som leveransen omfattar.

• Uppgifterna ska lagras krypterade eller vara pseudonymiserade så att leverantör inte har åtkomst till identiteterna.

• Data ska vara krypterad i vila och under transport (insynsskyddat).

• Åtkomst får bara ske efter tillåtelse från Region Skåne (t.ex. åtkomst sker bara i anledning av initierat supportärende).

• Att radering verkligen sker (särskilt vad avser backuper).

• Att anställda ingår avtal om tystnadsplikt (enbart att leverantören ingått avtal om tystnadsplikt har av JO inte ansetts vara tillräckligt skydd för att uppgifterna inte ska anses vara röjda, se JO beslut 2014-09-09, dnr 3032-2011.)

Vem får skriva under ett biträdesavtal i Region Skåne?

Det finns i Region Skåne inga särskilda delegeringar avseende just biträdesavtal. Den som har delegation att skriva under själva huvudavtalet är därför den som även ska skriva under biträdesavtalet. Biträdesavtalet bör ses som en del av huvudavtalet och också diarieföras och hanteras tillsammans med detta avtal.

BILAGA 1

Checklista för förberedelse innan ett personuppgiftsbiträde anlitas

Enligt Dataskyddsförordningen får personuppgiftsbiträden bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Normalt utformar den personuppgiftsansvarige själv instruktionerna. När man anlitar en stor extern leverantör, som t.ex en molntjänstleverantör, är man däremot ofta hänvisad till de villkor som gäller enligt leverantörens standardavtal. I sådana fall måste den personuppgiftsansvarige granska de avtalsvillkor och riktlinjer som leverantören erbjuder och göra en bedömning utifrån dessa. Bedömningen måste göras utifrån Dataskyddsförordningens bestämmelser och slutsatserna av den personuppgiftsansvariges egen risk- och sårbarhetsanalys.

Den personuppgiftsansvarige måste bland annat:

- **ta ställning till om det finns risk för att personuppgifter kan komma att behandlas för andra ändamål än de ursprungliga**
  Kommentar: [Utrymme för kommentar]. Exempel på kommentar: avtalet innehåller bestämmelser om att biträdet kan använda personuppgifterna för egna ändamål, såsom marknadsföring, vidareutveckling av egna tjänster eller i övrigt för att främja sin affärsmodell.

- **ta ställning till om leverantören kan komma att behandla personuppgifter i ett så kallat tredjeland, det vill säga ett land utanför EU/EES, och om den överföringen i så fall har stöd i Dataskyddsförordningen**
  Kommentar: [Utrymme för kommentar]. Exempel på kommentar: avtalet innehåller bestämmelser om att support kommer att ske från land utanför EU. Det innebär att personuppgifterna kommer att behandlas i ett land utanför EU/EES.

- **bedöma vilka säkerhetsåtgärder som måste vidtas för att skydda de personuppgifter som behandlas**
  Kommentar: [Utrymme för kommentar] Exempel på kommentar: Dataskyddsförordningen ställer generella krav på att nödvändiga säkerhetsåtgärder måste vidtas både tekniskt och organisatoriskt. I avtalet och instruktioner kan den personuppgiftsansvarige specificera en del generella åtgärder som leverantören ska vidta. Mer exakt vilka åtgärder som ska vidtas måste den personuppgiftsansvarige organisationen bedöma, lämpligen genom en riskanalys där man går igenom såväl vilka uppgifter som omfattas av tjänsten, vilka risker som finns och vilka åtgärder som måste vidtas för att minimera dessa risker. Det faktum att känsliga personuppgifter och uppgifter som omfattas av sekretess kommer att hanteras i systemet ställer vissa grundkrav som följer av Socialstyrelsens föreskrifter; säker autentisering (tvåstegsautentisering) för åtkomst till uppgifterna och att alla överföringar i nätverk måste ske krypterat.

- **se till att ett personuppgiftsbiträdesavtal upprättas med molnleverantören samt**
  Kommentar: [Utrymme för kommentar, det finns nedan en checklista för att kontrollera biträdesavtalet]

- **bedöma att personuppgiftbiträdet ger tillräckliga garantier och faktiskt har möjligheter att behandla personuppgifterna med tillräckliga tekniska och organisatoriska åtgärder för att skydda dem (artikel 28 1, Dataskyddsförordningen)**
  Kommentar: [Utrymme för kommentar, det finns nedan en checklista för att kontrollera biträdesavtalet]

- **beakta annan lagstiftning, till exempel sekretesslagstiftning.**
  Kommentar: [Utrymme för kommentar] Exempel på kommentar: Det finns en problematik i att överföra uppgifter som omfattas av sekretess till en tjänstetillhandahållare utanför myndigheten, nämligen att uppgifterna som omfattas av sekretess kan anses vara röjda för tjänstetillhandahållaren. Offentlighets- och sekretesslagen förbjuder myndigheter från att obehörigen röja sekretesskyddat material. Om information kan vara krypterad så skulle det kunna utgöra en lösning, då anses informationen inte vara röjd under förutsättning att kryptering innebär att montjänstleverantören inte kan ta del av uppgiften. En annan lösning är pseudonymisering, dvs. att skarpa personuppgifter inte hanteras i systemet utan någon form av kodning sker.

Riskanalys

En personuppgiftsansvarig är fortfarande ansvarig för personuppgifterna när de hanteras av ett biträde. Det innebär att den ansvarige måste säkerställa att biträdet kan hantera uppgifter på ett säkert sätt. Med säkert avses såväl utifrån en teknisk synpunkt som från en organisatorisk och legal synpunkt. Det ligger alltså i den personuppgiftsansvariges skyldighet att inte bara ställa krav utan även utreda vilka krav som måste ställas samt skapa sig en uppfattning om huruvida dessa krav kan uppfyllas. Ett lämpligt sätt att genomföra detta är att genomföra en riskanalys i god tid innan tjänsten upphandlas eller tas i bruk. En riskanalys ska belysa och värdera de risker som kan finnas och föreslå åtgärder för att minimera dessa risker. Av Socialstyrelsens föreskrifter (3 kap. 5 § HSLF-FS 2016:40) framgår att löpande riskanalyser ska ske för att utreda huruvida någon av de krav som Socialstyrelsen ställer kan komma att brytas emot. Genom Dataskyddsförordningen finns det ett krav om att riskanalyser (konsekvensbedömningar) genomförs innan personuppgiftbehandlingar påbörjas om behandlingen i sig kan anses vara känslig (t.ex. omfatta stor mängd känsliga personuppgifter eller på ett riskfyllt sätt hantera personuppgifter). Det finns således krav i flera lagstiftningar om att riskanalys genomförs.

Riskanalyser ska alltid vara skriftliga och utgör även ett beslutsunderlag som beslutsfattaren kan grunda sitt beslut om att gå vidare med en upphandling eller implementering av ett IT-stöd på. Det är mycket viktigt att ett beslut om att överföra uppgifter till ett personuppgiftsbiträde sker informerat, dvs. att beslutsfattaren förstår innebörden och de risker detta kan medföra.

Bilaga 2

Checklista för bedömning av externt biträdesavtal

Det måste finnas ett skriftligt biträdesavtal. I det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i (enligt art 28 i Dataskyddsförordningen).

Uppfyllt? [Ja / nej]

Följande punkter ska framgå av biträdesavtalet:

„ . Framgår att biträdet är skyldigt att tillämpa Dataskyddsförordningen och i övrigt Svensk lagstiftning när det gäller behandling av de personuppgifter som omfattas av avtalet.
Uppfyllt? [Ja / nej]

„ . Framgår föremålet för behandlingen (vad det är för personuppgifter som ska behandlas, vilka kategorier av registrerade som återfinns) (jmfr art 28 p 3 i Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . Framgår om det är särskilt känsliga personuppgifter (ingår känsliga personuppgifter (definierat i lagstiftning art 9 p 1 Dataskyddsförordningen) eller extra skyddsvärda (som av sitt sammanhang eller sin karaktär är extra skyddsvärda) (jmfr art 28 p 3 i Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . Framgår behandlingens varaktighet (tidsbestämt eller tills vidare) (jmfr art 28 p 3 i Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . framgår att personuppgiftsbiträdet är skyldigt att vidta lämpliga säkerhetsåtgärder (enligt art 32 i Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . framgår att personuppgiftsbiträdet endast får behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner och därmed säkerställa att personuppgiftsbiträdet inte behandlar personuppgifter för andra ändamål än dem som personuppgiftsbiträdet anlitats för (Art 29 Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . framgår att personuppgiftsbiträdet endast får överföra personuppgifter till ett land som ligger utanför EU och som saknar tillräckligt legala skydd för hanteringen av personuppgifter (s.k. tredje land) om det finns uttryckliga instruktioner om detta från personuppgiftsansvarig. (Art 28 p 3 a, Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . säkerställa att den personuppgiftsansvarige notifieras innan underbiträden anlitas (underbiträden till personuppgiftsbiträdes som kan komma att behandla den personuppgiftsansvariges personuppgifter) (enligt art 28 p 3 d, Dataskyddsförordningen). Observera att det inte är någon självklarhet att underbiträden ska utnyttjas. Den personuppgiftsansvarige kan mycket väl villkora att inga underbiträden ska finnas. Om inget skrivs om det i avtalet så finns det inte någon rätt att anlita underbiträden (enligt art 28 p 1 Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . säkerställa att de eventuella underbiträden som avses ovan villkoras med samma skyldigheter som personuppgiftsbiträdet har (enligt art 28 p 4, Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . säkerställa att den personuppgiftsansvarige på lämpligt sätt har möjlighet att följa upp att personuppgiftsbiträden lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen vidtar lämpliga säkerhetsåtgärder, t.ex. genom möjlighet till revision. (enligt art 28 p 3 c, Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet (avtal om tystnadsplikt) eller omfattas av en lämplig lagstadgad tystnadsplikt, (Art 28 p 3 b, Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstankar om att någon hos den personuppgiftsansvarige eller hos något personuppgiftsbiträde haft obehörig åtkomst till personuppgifterna
Uppfyllt? [Ja / nej]

„ . villkor om att biträdet ska understödja den personuppgiftsansvarige med det som behövs för att tekniskt möjliggöra att den personuppgiftsansvarige hanterar de registrerades rättigheter (som t.ex. registerutdrag, radering av personuppgifter, rättelse m.m.), (Art 28 p 3 e, Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . personuppgiftsbiträdet ska notifiera Region Skåne snarast vid händelse av personuppgiftincident. Samt i övrigt stödjer den personuppgiftsansvarige med anmälan av en personuppgiftsincident till tillsynsmyndigheten samt i förekommande fall till registrerade. (art 28 p 3 f, Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

„ . Ansvar för skada / skadeståndsbegränsning. Finns bestämmelser i avtal om hur krav på ersättning för skada (eller om en behörig myndighet utfärdar vite eller andra administrativa påföljder) med anledning av personuppgiftsbehandling? I Region Skånes standardavtal står att om personuppgiftsbiträde gör något i strid med instruktioner, detta avtal eller gällande dataskyddsregler ska personuppgiftsbiträde hålla personuppgiftsansvarig skadeslös. [ytterst är

skadeståndsbegräsningar en förhandlingsfråga, men det är för personuppgiftsansvarig viktigt att det är tydligt vad som gäller om biträdet bryter mot de krav som ställts i avtalet. Eftersom både personuppgiftsansvarig och personuppgiftsbiträde har ansvar enigt Dataskyddsförordningen så kan skadestånd från registrerad riktas mot vilken som helst av parterna. Finns den tydlighet i avtalet kring skadeståndsansvar blir det lättare att rikta regresskrav mot motparten (alltså att personuppgiftsansvarig, efter att denne betalt skadestånd till registrerad kan rikta krav mot personuppgiftsbiträdet som varit den som gjort något otillåtet)]
Uppfyllt? [Ja / nej]

„ . säkerställa att parterna vet vilka åtgärder (raderande eller återlämning till personuppgiftsansvarig) som ska vidtas vid avtalets upphörande så att personuppgiftsbiträdet inte har åtkomst till personuppgifterna därefter. (Art 28 p 3 g, Dataskyddsförordningen)
Uppfyllt? [Ja / nej]

Bilaga 3

Exempel instruktion för hantering av Personuppgifter

Nedanstående är ett exempel på instruktion till biträdet som kan användas vid biträdesavtal.

Utöver vad som redan framgår av detta avtal ska Personuppgiftsbiträdet även följa nedanstående instruktioner:

Personuppgiftsbehandling	
Ändamål för behandling av personuppgifter *Specificering av samtliga ändamål för vilka personuppgifter som kommer behandlas av PuB.*	Här ska framgå för vilka ändamål som personuppgifter kommer att behandlas. T.ex. PuB kommer att behandla personuppgifter för ändamålet att tillhandahålla tjänsten i enlighet med Avtalet, dvs support. Praktiskt rör det sig om att PuB kan behöva se patientinformation för att lösa användarproblem.
Kategorier av personuppgifter *Specificera kategorier av personuppgifter som kommer behandlas av PuB.*	Här ska framgå vilka kategorier av personuppgifter som kommer att behandlas. T.ex. De personuppgifter som kommer att behandlas kan inkludera personuppgifter tillhörande följande kategorier: 1) Personuppgifter hänförliga till den Personuppgiftsansvariges personal, i huvudsak kontaktuppgifter; 2) Personuppgifter hänförliga till den Personuppgiftsansvariges patienter, inklusive hälsorelaterade och potentiellt känsliga uppgifter; och Personnummer Sjukfrånvaro/frånvaro Patientuppgifter
Känsliga personuppgifter *Ange vilka särskilda kategorier av personuppgifter som behandlas*	Här ska framgå om särskilda kategorier av personuppgifter enligt (definierat i art 9 p 1 Dataskyddsförordningen) ingår i behandlingen eller om det förekommer andra personuppgifter som är särskilt skyddsvärda. T.ex. Journalhandlingar i form av remiss, anamnes, bilder och svar.
Kategorier av registrerade	Här ska kategorier av registrerade framgå. T.ex. Kategorierna av registrerade inkluderar:

Specificera samtliga kategorier av registrerade vars uppgifter kommer behandlas av PuB.	1) Patientuppgifter såsom remiss, anamnes, bilder och svar.
Överföring av personuppgifter *Den omfattning som personuppgifter kan komma att överföras utanför EES i syfte att tillhandahålla tjänsterna enligt avtalet.*	Specificera om personuppgifter kommer att överföras utanför EU/EES i anledning av tjänsten. Som en del av Personuppbiträdets fullgörande av tjänsterna som levereras enligt Tjänsteavtalet kan *avidentifierade* personuppgifter relaterade till supportärenden samt personuppgifter i form av kontaktuppgifter såsom namn, telefonnummer och e-postadress hänförliga till den Personuppgiftsansvariges personal komma att föras över till Personuppbiträdets underleverantör, se Bilaga X.
Arkivering och gallring *Specificera gallringstid avseende när personuppgifterna som behandlas av PuB ska gallras.*	Eventuella instruktioner till PuB vad avser arkivering och gallring av personuppgifter.
Återlämning av data *Ange hur PuB ska lämna tillbaka data efter avslutande behandling av personuppgifter*	Eventuella instruktioner om hur återlämning av personuppgifter och annan data ska ske.
Informationssäkerhet och IT-säkerhet *Ange de specifika krav som har tagits fram vid genomförande av informationsklassning*	Eventuella specifika krav av avser Informationssäkerhet eller IT-säkerhet. Detta kan vara redan specificerat i annan del av avtalet och en hänvisning kan vara tillräcklig.
Särskilda instruktioner om behandlingen *T.ex. om vissa uppgifter ska beaktas särskilt (skyddade personuppgifter m.m.)eller om behandlingen av vissa uppgifter ska utföras på ett särskilt sätt*	Eventuella särskilda instruktioner kring behandling. Kan till exempel avse att endast vissa individer får ha åtkomst till uppgifter. Att åtkomst får ske endast under vissa förutsättningar. Att alla personuppgifter ska förvaras krypterade. Personuppgiftsbiträdet får endast ha åtkomst till personuppgifter i samband med ett supportärende som initierats av personal tillhörig den personuppgiftsansvarige.