



DATAOMBUDSMANNENS BYRÅ

**UTKONTRAKTERING AV
PERSONUPPGIFTSBEHANDLING, GEMENSAMMA
DATASYSTEM, SAMVERKAN I NÄTVERK OCH
TILLHÖRANDE AVTAL**

Uppdaterad 27.07.2010

www.tietosuoja.fi

INNEHÅLL

I	Inledning	3
II	Planering och hantering av utkontraktering i fråga om personuppgiftsbehandling....	3
III	Gemensamma datasystem/personuppgiftsbehandling i nätverkssamverkan	8
IV	Exempel	11

BILAGOR

Bilaga 1: Mall för ett skriftligt uppdragsavtal (avtalsstruktur)

Bilaga 2: Checklista med exempel på vilka/vilken typ av frågor som bör fastställas i ett uppdragsavtal

BILDER

Bild 1. Exempel, översiktlig beskrivningsmodell för behandlingen av personuppgifter (tabell, sidan 6)

Bild 2. Exempel på ett datasystem som planerats för administration av ett personregister med ändamålet XX (sidan 7)

Bild 3. Gemensamt datasystem/nätverksbaserat datasystem ämnat för flera myndigheters bruk (sidan 11)

Bild 4. Exempel på parter, aktörer och element i ett regionalt datasystem inom hälso- och sjukvården (sidan 12)

UTKONTRAKTERING AV PERSONUPPGIFTSBEHANDLING, GEMENSAMMA DATASYSTEM, SAMVERKAN I NÄTVERK OCH TILLHÖRANDE AVTAL

I Inledning

Ett centralt syfte med personuppgiftslagen är att åstadkomma god informationshantering och därmed också god databehandling. Detta förutsätter framför allt omsorgsfull förhandsplanering.

I denna broschyr redogörs med hjälp av exempel kort för de centrala krav i personuppgiftslagen som skall beaktas då sådana funktioner som förutsätter behandling av personuppgifter utkontrakteras eller datasystem sammanbinds i nätverk samt då avtal om detta upprättas. Beslut om datasystem och utkontraktering fattas i sista hand av organisationens ledning. Av denna anledning riktar sig broschyren särskilt till ledningen för dessa projekt och den personal som deltar i utvecklingen och planeringen av funktioner och databehandlingssystem.

II Planering och hantering av utkontraktering i fråga om personuppgiftsbehandling

Vid utkontraktering av funktioner som förutsätter behandling av personuppgifter skall i planeringsskedet särskilt kraven i personuppgiftslagen (523/1999) beaktas vid sidan av annat relevant. I praktiken kan till exempel databehandlingstjänster som gäller personuppgifter utkontrakteras för den registeransvariges räkning som beställer tjänsterna. I detta fall upprättas ett uppdragsavtal mellan den registeransvarige som beställer tjänsterna (uppdragsgivaren) och den som tillhandahåller tjänsterna (uppdragstagaren). Den registeransvarige i fråga ansvarar då för att databehandlingen liksom också den övriga verksamheten utförs lagenligt. Serviceproducenten ansvarar för uppgiftsbehandlingen i enlighet med det uppdragsavtal som ingår parterna emellan. Sådan behandling av personuppgifter som utförs för en uppdragsgivares räkning på basis av avtal betraktas som användning av register. Att överlämna personuppgifter till en uppdragstagare för databehandling betraktas således inte som utlämnande av personuppgifter, vilket skulle kräva den berörda registrerades samtycke. Å andra sidan har uppdragstagaren inte rätt att i sin egen verksamhet använda de personuppgifter som denne fått inom ramen för ett uppdragsförhållande. Uppdragstagaren får inte heller behandla personuppgifter på ett sätt som strider mot avtalet eller foga uppgifter till annat material som denne förfogar över.

Med registeransvarig avses:

”en eller flera personer, sammanslutningar, inrättningar eller stiftelser för vilkas bruk ett personregister inrättas och vilka har rätt att förfoga över registret eller vilka enligt lag ålagts skyldighet att föra register” (3 kap. 1 § punkt 4 PuppL)

Att anskaffa databehandlingstjänster från ett utomstående företag innebär ökade och annorlunda datasäkerhets- och dataskyddsrisker. Därför är det viktigt att det i avtalet fastställs tillräckligt detaljerat vilka olika behandlingsprocesser och uppgifter serviceproducenten utför och ansvarar för samt vilka uppgifter och ansvar som kvarstår hos beställaren. I avtalet skall också definieras hur datasäkerheten tryggas i de olika behandlingsfaserna. Ur personuppgiftslagens perspektiv fullgör datasäkerheten i synnerhet den skyddsplikt som nämns i personuppgiftslagen. Kravet på planering och genomförande av datasäkerhet och skydd av uppgifter berör alla faser i behandlingen av personuppgifter.

Med tanke på fastställandet av ansvar är det viktigt att avtalets rättsliga karaktär konstateras klart och tydligt i avtalet (uppdragsavtal). I anslutning till detta skall det också noteras att enligt 5 kap. 2 § i lagen om offentlighet i myndigheternas verksamhet (621/1999, med senare ändringar) skall offentlighetslagen tillämpas på handlingar/uppgifter som upprättats på uppdrag av en myndighet. Även detta skall konstateras i uppdragsavtalet.

För att utkontrakteringen och avtalet skall utfalla väl förutsätts det att företaget, sammanslutningen, myndigheten eller någon annan registeransvarig är förtrogen med och behärskar processerna i anslutning till den funktion som utkontrakteras och att vederbörande har bedömt all behandling av uppgifter som utförs inom ramen för verksamheten utgående från kraven i personuppgiftslagen. I relation till detta förutsätts att

- Den registeransvarige har kartlagt och beskrivit sitt dokumentmaterial samt angett vilka alla personregister som uppkommer för olika ändamål i den registeransvariges verksamhet.
- Den registeransvarige har också gjort upp en beskrivning över det personregister som kommer att användas i den funktion som enligt planerna skall utkontrakteras, processerna i anslutning till registerföringen och den behandling av personuppgifter som funktionen förutsätter.
- Beskrivningen har uppgjorts med beaktande av funktionella, tekniska och lagenliga krav, varvid uppgifterna behandlas på ett sätt som är förenligt med bestämmelserna om god informationshantering i personuppgiftslagen och offentlighetslagen. Detta innebär till exempel att onödiga och oriktiga uppgifter inte får samlas in eller lagras samt att uppgifterna skall behandlas med iakttagande av aktsamhets- och skyddsplikten, kravet på ändamålsbundenhet och plikten att tillgodose de registrerades rättigheter.

Exempel på olika funktioner (ändamål) i samband med vilka personregister bildas:

1. Vid hanteringen av olika kundförhållanden i företag, banker och försäkringsanstalter bildas kundregister.
2. I samband med uppgifter som ålagts kommunen i lag och den hantering av kundförhållanden som dessa förutsätter bildas olika personregister för varje uppgift (t.ex. elevregister vid anordnande av undervisning, klientregister i olika uppgifter inom socialvården).
3. De lagstadgade uppgifter som handhas av statens myndigheter förutsätter ofta insamling av personuppgifter. (T.ex. Statskontoret handhar lagstadgade uppgifter såsom de statsanställdas pensionsärenden och statens olycksfallsärenden.) I samband med varje uppgift bildas ett personregister för ett bestämt ändamål för att uppgiften i fråga skall kunna utföras.
4. Organisationerna inom såväl den offentliga som den privata sektorn behöver följande register för ärenden i samband med anställning och personaladministration:
 - a) register för personaladministration
 - b) register över arbetssökande

Det bör i samband med planeringen noteras att alla de uppgifter som behandlas för att uppdraget i fråga skall kunna utföras hör till ett och samma personregister (registrets

användningsändamål). God informationshantering förutsätter att en beskrivning uppgörs över den helhet som bildas inom ramen för en bestämd funktion som handhas av den registeransvarige (logiskt personregister). Även om ett datasystem kan delas in i delfunktioner, förutsätter behovsplaneringen, genomförandet och också utkontrakteringen av verksamheten och databehandlingen att planeringen utgår från en helhetsbild av funktionen och dess olika delfunktioner, processer och arbetsflöpp.

Med personregister avses:

”en datamängd som innehåller personuppgifter och som består av anteckningar som hör samman på grund av sitt användningsändamål, och som helt eller delvis behandlas med automatisk databehandling eller har ordnats som ett kartotek, en förteckning eller på ett annat motsvarande sätt så att information om en bestämd person kan erhållas med lätthet och utan oskäligen kostnader” (3 § 1 mom. 3 punkten PuppL).

”Ändamålet med behandlingen av personuppgifter skall preciseras så att av det framgår för vilka av den registeransvariges funktioner personuppgifter behandlas” (6 § 2 mom. PuppL).

Utkontraktering kan ske på olika sätt, till exempel så att

- en myndighet, ett företag eller någon annan sammanslutning (den registeransvarige) anskaffar databehandlingstjänster eller andra tjänster av ett privat företag
- en statlig eller kommunal myndighet anskaffar databehandlingstjänster och andra tjänster av en annan myndighet.

När man planerar att utkontraktera funktioner och tillhörande personuppgiftsbehandling skall utkontrakteringen beskrivas som en del av registerföringen i anslutning till funktionen i fråga.

- I detta sammanhang planeras i detalj vilka funktioner och ansvar i anslutning till personuppgiftsbehandlingen som den eventuella serviceproducenten förutsätts ta hand om och vilka funktioner som den registeransvarige fortsättningsvis ansvarar för, vilka eventuella risker och hot som arrangemangen medför och hur dessa kan avhjälpas, hur olika förfaranden skall utföras, samt vad serviceproducenten förutsätts ta i beaktande för att kraven på datasäkerhet och dataskydd skall uppfyllas i de olika behandlingsfaserna.
- I alla faser skall det säkerställas att ingens integritet omotiverat äventyras. Detta förutsätter bland annat att datastrukturerna skall planeras och genomföras så att rättigheterna att använda personuppgifterna begränsas till sådana uppgifter som är relevanta för respektive funktion, samt att personuppgifter inte utlämnas – där detta är tillåtet i lag – i större utsträckning än vad som är nödvändigt för ändamålet i fråga. Vid planeringen av dokument, skärmbilder och vyer skall säkerställas att inga onödiga uppgifter anges i dessa (t.ex. personbeteckning).
- Omsorgsfull planering och beredning garanterar att de anbudsfrågningar och avtal som krävs i ärendet kan utarbetas tillräckligt detaljerat. När det gäller avtal skall parternas uppgifter och ansvar beskrivas och fastställas tillräckligt detaljerat, så att det står klart vad som har avtalats och det är möjligt att ingripa vid eventuella avtalsbrott.
- Det är också viktigt att förutse och i avtalet fastställa vilka situationer som kan leda till att avtalet upphör samt vilka uppgifter och förpliktelser parterna har att fullfölja i detta sammanhang.

Tabellen nedan anger på vilket sätt den registeransvarige skall beskriva och bedöma registerföringens funktion och lagenlighet. (Bild 1)

Om den registeransvarige överväger utkontraktering, skall det i planeringsskedet beskrivas vilka av den registeransvariges funktioner/delfunktioner och därtill anslutna personuppgiftsbehandlingsprocesser som enligt planerna kommer att utkontrakteras. Varje behandlingsfas är också förknippad med krav på dataskydd och datasäkerhet. Planeringen skall utföras som ett logiskt register så att behandlingen av och arbetsförloppen för allt material som uppkommer inom ramen för funktionen i fråga (datamaterial och manuellt material) inkluderas i beskrivningen.

Bild 1: ÖVERSIKTLIG BESKRIVNINGSMODELL FÖR BEHANDLINGEN AV PERSONUPPGIFTER

REGISTERANSVARIG: (3 § 1 mom. 4 punkten PuppL) T.ex. <i>centrala ämbetsverket xx</i>					
REGISTRETS ANVÄNDNINGSSÄNDAMÅL: (3 § 1 mom. 3 punkten och 6 § PuppL)			T.ex. <i>xx:s register för personaladministration</i>		
Behandlingsfas	Beskriv de behandlingsbehov verksamheten förutsätter per genomförandefas Per delfunktion +ansvar	Beskriv och bedöm riskerna för och hoten mot dataskyddet i varje behandlingsfas	Definiera behandlingsförfarandena samt hur datasäkerheten och dataskyddet tillgodoses i varje fas/delfunktion - vem gör? - vad görs? - på vilket sätt?	Definiera och säkra de rättsliga förutsättningarna för behandlingen och förfarandena - utvärdering per behandlingsfas enligt PuppL och eventuella specialbestämmelser	Funktioner och ansvar som enligt utkontrakteringsplanerna skall utföras av en serviceproducent
Insamling av uppgifter/ Datainnehåll - typ av uppgifter - källor/ grund för erhållande av information, m.m.				- 9 § PuppL - lagen om integritetsskydd i arbetslivet - eventuella specialbestämmelser	
Internt bruk och skydd av registret, inkl. Datasäkerhet				- 5 och 32 § PuppL - eventuella specialbestämmelser (t.ex. 18 § OffL)	
Utlämnande - till vem? - i vilket syfte? - vilka uppgifter? - på vilken grund?				- 8 §, 12 §, 5 §, 9 §, 32 § PuppL - eventuella specialbestämmelser (t.ex. 16 § 3 mom. OffL)	
Förvaring och förstöring - förvaringstid * aktiv/ passiv tid - tillvägagångssätt				- 34 §, 5 §, 9 §, 32 § PuppL - eventuella specialbestämmelser (t.ex. arkivlagen)	
Information till de registrerade - om vad? - hur?				- 24 §, 3 § 1 mom. 7 punkten PuppL - lagen om integritetsskydd i arbetslivet - eventuella specialbestämmelser	
De registrerades rättigheter				- 26–29 § PuppL, - eventuella specialbestämmelser	

- rätt till insyn - rättelse av fel - förbuds rätt					
Övriga beskrivningar av nödvändiga behandlingsfaser				- 5 §, 9 §, 32 § Puppl - 16–23 § lagen om integritetsskydd i arbetslivet	

På följande bild presenteras ur en annan synvinkel den helhet och de olika element som skall fastställas och beskrivas i behandlingen av personuppgifter och i planeringen och genomförandet av det datasystem som utnyttjas för behandlingen (Bild 2). Samma aspekter skall bedömas också när det gäller en serviceproducents verksamhet, dock med beaktande av de funktioner och behandlingsprocesser som utkontrakterats.

Bild 2:

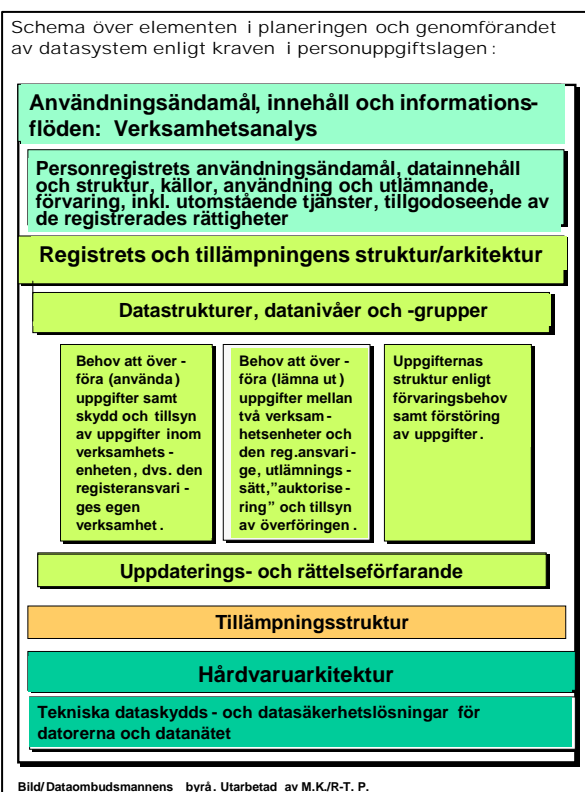
Exempel på de olika elementen i ett datasystem som planerats för administration av ett personregister med ändamålet XX.

LOGISKT REGISTER =

- behandling som utförs av den registeransvariga organisationen själv
- behandling som utförs av en utomstående serviceproducent för den registeransvariges räkning på basis av ett uppdragsavtal
→ behandlingen är en del av den registeransvariges logiska personregister

Den registeransvariges egen verksamhet:

Funktioner som ämnas utföras av en serviceproducent (uppdragstagare):



Beskrivning och analys över funktioner och ansvar som ämnas överföras på uppdragstagaren, bl.a.

- funktioner som berör användning och annan behandling, t.ex. utlämnande, av personuppgifter
 - *
 - *
 - *
- funktioner, krav och ansvar i anslutning till datasäkerhet och dataskydd
- krav och ansvar i anslutning till datautrustning o.d.
- sekretesskrav och andra krav som berör personalen
 - * sekretess- och användarförbindelse
- andra funktioner och ansvar som berör uppgiftsbehandling (t.ex. informering och tillgänglighållande av registerbeskrivning)

←
UPPDRAGS-
AVTAL



Skyldigheten att trygga datasäkerheten gäller alla behandlingsfaser och alla nivåer och delar i genomförandet av ett datasystem.

Som bilaga 1 följer en mall till ett uppdragsavtal och som bilaga 2 en checklista, där det räknas upp exempel på vad/vilka typer av ärenden som skall fastställas i ett uppdragsavtal.

III Gemensamma datasystem/personuppgiftsbehandling i nätverkssamverkan

Med gemensamt datasystem avses här ett data- eller dataöverföringssystem som två eller flera självständiga företag, institutioner, myndigheter o.d. (registeransvariga) utarbetat tillsammans för att bättre kunna sköta sina uppgifter och funktioner.

I sådana fall där funktionerna förutsätter och/eller innefattar också behandling av personuppgifter, skall utarbetandet av datasystem alltid bedömas också med tanke på personuppgiftslagstiftningen. Det är viktigt att notera att de olika registeransvarigas personregister inte får sammanföras i ett gemensamt datasystem/datasystem i sambruk. Det att flera registeransvariga ansluter sig till gemensamma datasystem eller dataöverföringssystem/nätverk ändrar således inte det ansvar som gäller för de enskilda registeransvariga vid behandling av personuppgifter (registerföring). För den registeransvarige, till exempel en myndighet, handlar det om att verksamhetsmiljön, tekniken och arbetssätten i anslutning till uppgiftsbehandlingen ändras. Datasystemet är ett hjälpmedel, med vars hjälp personuppgifter som ingår i den registeransvariges/de registeransvarigas personregister kan överföras, förvaras, utlämnas och i övrigt behandlas. (Registeransvarig, personregister och personuppgiftsbehandlingens (registrets) användningsändamål definieras på sidorna 3 och 5.)

Precis som vid anlitan av utomstående tjänster är det viktigt att analysera och på förhand planera frågor och krav i anslutning till användningen av ett gemensamt data- och dataöverföringssystem eller nät. Också här är utgångsläget att varje registeransvarig som deltar i projektet (myndighet, företag e.d.) är förtrogen med sina egna funktioner och behärskar de processer, den databehandling och de arbetssätt som hänför sig till dessa, och följaktligen kan bedöma vad ett nätverkssamarbete förutsätter med tanke på den egna verksamheten. Bedömningen skall utgå ifrån såväl de funktionella behoven som de tekniska (bl.a. datasäkerhetsfrågor) och rättsliga kraven (se bild 1 på sidan 6 och bild 2 på sidan 7).

Gemensamma datasystem förutsätter också gemensamt uppgjorda planer, där projektets genomförande beskrivs och bedöms utifrån verksamheten, lagstiftningen, det tekniska utförandet samt också kostnaderna. Vid införandet av ett datasystem är det viktigt att samarbetet mellan de deltagande registeransvariga (företag, sammanslutningar, myndigheter osv.) och deras ansvar har fastställts, att verksamheten är planmässig och koordinerad samt att alla avtal som krävs har upprättats med fastställda ansvar. Planeringen förutsätter bland annat dels separata beskrivningar över varje registeransvarigs aktuella personregister och behandlingen av personuppgifter i anslutning därtill, dels en beskrivning över projektet som helhet och deltagarna samt den behandling av personuppgifter som hänför sig till projektet och behoven i relation till behandlingen. Det skall finnas en ändamålsenlig beskrivning över alla processer och arbetsförlopp som utförs inom ramen för projektet, så att de mål och krav som fastställts för detsamma skall kunna bedömas och uppfyllas (bild 4 på sidan 12), och så att projektets lagenlighet skall kunna säkerställas i alla behandlingsfaser.

Den registeransvarige skall bland annat vara förtrogen med informationsflödena i anslutning till sina olika funktioner; från vilka källor uppgifter i regel och även annars insamlas och behöver

insamlas, vart uppgifter i regel behöver lämnas ut och vilken typ av uppgifter som i praktiken lämnas ut, samt på vilken lagstiftningsgrund uppgifter kan insamlas och utlämnas.

När man planerar att lämna ut och överföra personuppgifter ur ett personregister till en annan organisation elektroniskt via ett nät ska man se till att de rättsliga förutsättningarna för utlämnande av uppgifter uppfylls. Särskilt viktigt är det också att sörja för att datasäkerhets- och dataskyddskraven samt felfrihetskravet uppfylls på det sätt som lagstiftningen förutsätter. Bland de krav som skall beaktas kan nämnas aktsamhets- och skyddsplikten samt relevans- och felfrihetskravet, vilka anges i 5, 9 och 32 § i personuppgiftslagen, kraven på god informationshantering enligt 18 § i lagen om offentlighet i myndigheternas verksamhet och den förordning som utfärdats med stöd av denna samt eventuella andra krav i någon annan speciallag som möjligtvis skall tillämpas i det aktuella fallet. Vidare krävs också att parterna tillsammans har fastställt regler i syfte att säkerställa att uppgifter utlämnas och insamlas i enlighet med de villkor som gäller för verksamheten i fråga och de förutsättningar som anges i lag. I praktiken förutsätter detta bland annat att datastrukturerna är förenliga och det tekniska utförandet kompatibelt samt att avtal har ingåtts där varje parts åtaganden och därtill anknutna registerföringsansvar har fastställts.

Ett gemensamt datasystem och dataöverföringssystem förutsätter ofta i praktiken också utomstående databehandlingstjänster. Oftast blir det aktuellt för parterna i projektet att med beaktande av kraven i lagstiftningen tillsammans planera och avtala om anlitan av utomstående tjänster och vilka ansvar detta medför. Eftersom den registeransvariges ansvar kvarstår oförändrade kan utomstående tjänster i praktiken endast anlitas separat för varje registeransvarigs räkning. Även om anlitaandet av tjänster och andra därtill hörande frågor planeras av alla registeransvariga tillsammans, skall varje registeransvarig ingå separata uppdragsavtal med den utvalda serviceproducenten angående behandlingen och registerföringen av uppgifter i de egna registren.

Det är också möjligt att avtala om att någon av de registeransvariga som medverkar i projektet (ett företag, en myndighet e.d.) underhåller datasystemet för de övriga medverkandes räkning (på uppdragsbasis). I så fall verkar den registeransvarige i fråga i två olika roller: dels som registeransvarig för sitt egna register, dels som uppdragstagare gentemot de övriga registeransvariga och för deras räkning. En uppdragstagare har inte rätt att i sin egen verksamhet använda uppgifter som denna behandlar i samband med uppdraget i fråga eller sammanföra uppgifter från olika uppdragsgivares (registeransvarigas) personregister.

Vanligen övergår man stegvis till elektronisk behandling och överföring av uppgifter, dvs. en delfunktion åt gången. Ju större regional omfattning det planerade data- och dataöverföringssystemet kommer att ha (ibland t.o.m. riksomfattande), desto viktigare är det att genomförandet baserar sig på en tillräckligt omfattande helhetsbeskrivning. Endast då kan man bedöma för vilken verksamhetsmiljö en eventuell dellösning görs och hur denna kommer att inverka på och fungera i de projekt och datasystem som senare skall genomföras. Annars finns det risk för att datasystemsprojektet misslyckas eller att onödiga överraskningar uppstår under utvecklingsarbetet och genomförandet. I värsta fall kan totalkostnaderna för projektet mångdubblas. Omsorgsfull planering på förhand garanterar givetvis inte en lösning på alla framtida problem, men leder sannolikt till avsevärt färre problem.

Om personuppgifter överförs från en registeransvarig till en annan med hjälp av ett datasystem skall först och främst de rättsliga förutsättningarna för utlämnandet anges. Vidare skall det säkerställas att bland annat datasäkerheten, felfrihets- och relevanskraven samt kravet på

ändamålsenligt skydd av uppgifterna uppfylls *både för den överförande och den mottagande partens del*.

Personuppgifter kan utlämnas från ett personregister endast om utlämnandet uppfyller de förutsättningar som anges i lagstiftningen. De mest centrala rättsliga förutsättningarna för utlämnande av uppgifter kan presenteras enligt följande:

Uppgifter i myndigheters personregister

- 1) offentliga uppgifter: den registrerades samtycke, 16 § 3 mom. i offentlighetslagen eller en uttrycklig bestämmelse i någon annan lag,
- 2) sekretessbelagda uppgifter: den registrerades samtycke eller en uttrycklig bestämmelse om myndigheters sekretessbelagda personuppgifter (26 §, 29 § och 16 § 3 mom. i offentlighetslagen).
(Se dataombudsmannens byrås broschyr "Om utlämnande av personuppgifter ur myndigheternas personregister")

Privata företag o.d.

När det gäller personregister som förs av privata registeransvariga är utlämnande av uppgifter i regel endast möjligt med den registrerades samtycke eller, i enlighet med 8 § i personuppgiftslagen, på grundval av någon annan bestämmelse i lag som berättigar till utlämnande av personuppgifter.

Anvisningar om begäran om samtycke för behandling av personuppgifter finns i dataombudsmannens byrås broschyr "Behandling av personuppgifter med den berördes samtycke".

Öppnande av en teknisk anslutning innebär de facto utlämnande av personuppgifter; till exempel om en myndighet ges rätt att med hjälp av en elektronisk förbindelse se på uppgifter i en annan myndighets personregister, betraktas detta som elektroniskt utlämnande av personuppgifter. Av denna anledning kan en teknisk anslutning till exempelvis en annan myndighets eller någon annan registeransvarigs sekretessbelagda uppgifter öppnas endast under förutsättning att en uttrycklig bestämmelse i lag ger rätt till detta, och dessutom skall rätten att lämna ut uppgifter grunda sig på lag (den registrerades samtycke eller en uttrycklig bestämmelse i lag).

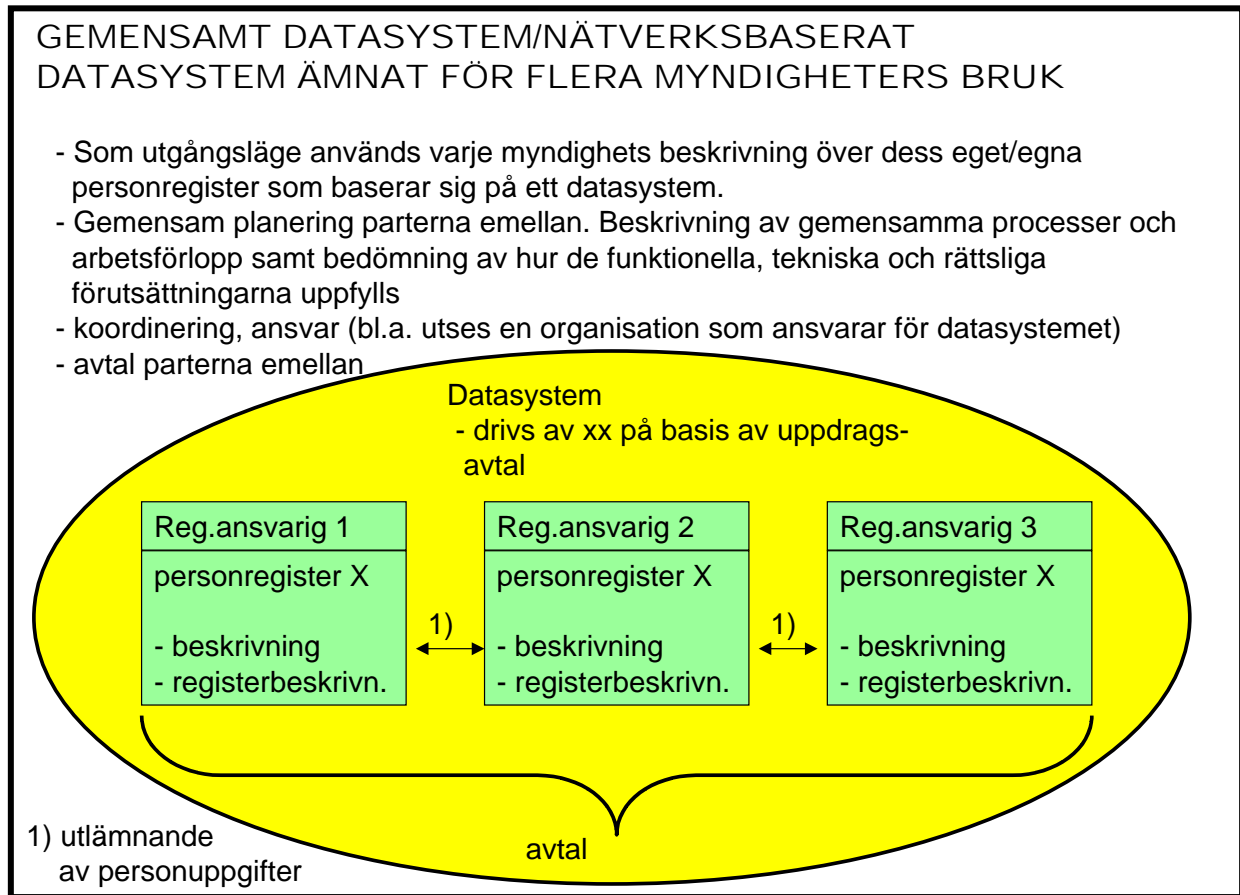
Riksdagens grundlagsutskott har i sina utlåtanden GrU 12 och 14/2002 rd konstaterat att det på lagnivå bör föreskrivas bland annat om öppnande av teknisk anslutning till en annan registeransvarig samt om förutsättningarna för detsamma.

Många lagar innehåller specialbestämmelser om öppnande av teknisk anslutning och dess förutsättningar. I 29 § i offentlighetslagen bestäms allmänt om myndigheters rätt att öppna en teknisk anslutning till uppgifter i personregister. Någon motsvarande allmän bestämmelse om privat verksamhet finns inte.

Även om en teknisk anslutning eller en anslutning som möjliggör att man kan se på uppgifter har öppnats i enlighet med ovan nämnda bestämmelser innebär det inte att vem som helst när som helst kan ges tillgång till eller tillåtelse att se på uppgifter i en annans registeransvarigs personregister med hjälp av anslutningen. Det skall alltid säkerställas med hjälp av tekniska metoder att uppgifterna är skyddade mot externt och obehörigt intrång enligt 32 § i personuppgiftslagen. Också kravet på ändamålsbundenhet enligt 7 § i personuppgiftslagen skall beaktas, vilket innebär till exempel att uppgifter inte får ses av nyfikenhet, utan endast om en

laglig rätt att behandla uppgifter föreligger med hänsyn till verksamheten och med stöd av personuppgiftslagen eller någon annan lag. Beviljande av rätt att se på uppgifter med stöd av någon lag eller någon annan möjlighet att lämna ut uppgifter med hjälp av en teknisk anslutning förutsätter å andra sidan också ett effektivt och planmässigt system för uppföljning och övervakning av utlämnande (t.ex. att man ser på uppgifter). Sådant system är ett loggsystem med tillhörande uppföljnings- och övervakningssystem. Att de lagstadgade kraven uppfylls skall säkerställas redan i samband med att ett tillstånd i ärendet beviljas/avtal i ärendet ingås. En registeransvarig som lämnar ut personuppgifter ur ett personregister ansvarar för att utlämnandet är lagenligt.

Bild 3: Gemensamt datasystem/nätverksbaserat datasystem ämnat för flera myndigheters bruk



IV Exempel

- 1) Många ministerier/förvaltningsområden har grundat eller har för avsikt att grunda servicecentraler med uppgiften att bistå förvaltningsområdets ämbetsverk i ärenden som gäller personaladministration och ekonomiförvaltning.

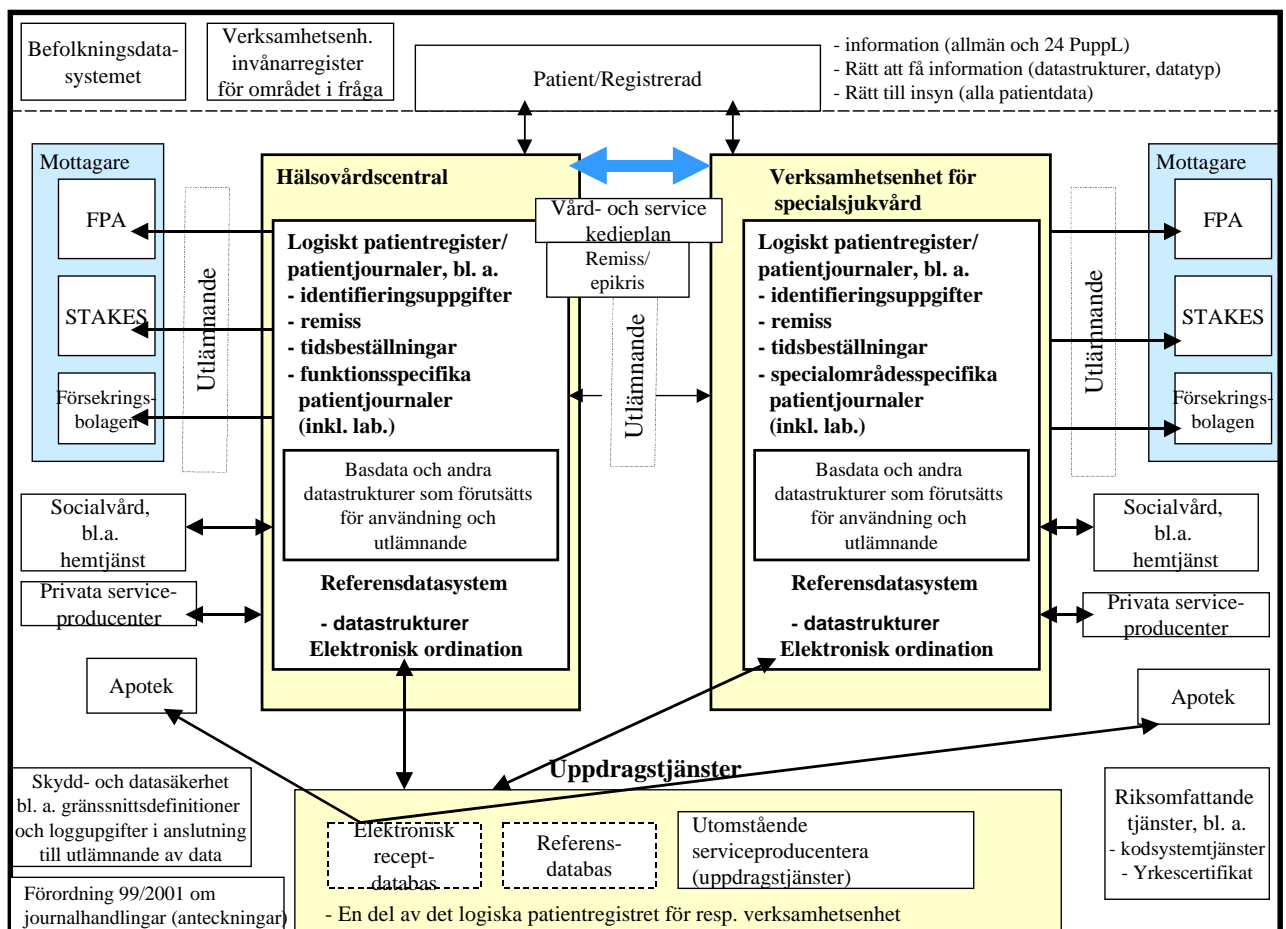
Varje myndighet som anlitar servicecentralens tjänster och det planerade datasystemet ansvarar fortsättningsvis i egenskap av registeransvarig till exempel för registerföringen av sin egen personaladministration. Om det inte finns några särskilda bestämmelser i lag om servicecentralerna och deras ansvar och uppgifter, ansvarar servicecentralen för behandlingen av personuppgifter på basis av avtalsansvar. Därtill skall servicecentralen med direkt stöd av lagen iakttä aktsamhets- och skyddsplikten enligt 5 och 32 § i personuppgiftslagen samt relevanta sekretessbestämmelser.

Servicecentralen och varje enskild myndighet skall således ingå ett separat uppdragsavtal, där myndighetens (uppdragsgivarens) och servicecentralens (uppdragstagarens) uppgifter och ansvar konstateras och fastställs också när det gäller registerföring. Den myndighet som planerar och samordnar projektet bör ingå ett s.k. serviceavtal med servicecentralen. Också ansvaret för det datasystem som anskaffats

och inrättats för ändamålet i fråga skall fastställas entydigt (underhåll, funktion osv.).

- 2) Ansvar för befolkningsdatasystemets funktionsduglighet ligger enligt befolkningsdatalagen hos befolkningsregistercentralen. Befolkningsregistercentralen ingår erforderliga avtal om databehandlingstjänster med utomstående serviceproducenter. Ansvar för behandlingen av personuppgifter i befolkningsdatasystemet har i lag ålagts magistraterna och delvis också befolkningsregistercentralen.
- 3) En dataöverföringsportal mellan ett antal myndigheter kan byggas upp på basis av ett avtal med en utomstående serviceproducent. Varje registeransvarig skall genom avtal säkerställa att utlämnandet av uppgifter eller givandet av uppgifter ur vederbörandes egna personregister sker på lagenliga grunder i enlighet med personuppgiftslagen och andra lagar som gäller detta och den egna verksamheten (se bild 1 på sidan 6 och bild 2 på sidan 7). För genomförandet av ett system som detta kan det också bli aktuellt att anskaffa identifieringstjänster av en utomstående serviceproducent. Varje registeransvarig skall ingå uppdragsavtal med utomstående serviceproducenter om de personregister som ligger på vederbörandes eget ansvar (t.ex. avtal om portalens administration och identifieringstjänster).
- 4) Exempel på parter, aktörer och element i ett regionalt datasystem inom hälso- och sjukvården:

(Bild 4)



När det gäller regionala datasystems- och nätverksprojekt inom hälso- och sjukvården är det

nödvändigt att ha dels en helhetsbeskrivning av parterna i projektet, deras ansvar och ställning i projektet samt eventuella utomstående aktörer, dels beskrivningar över respektive parts registerföring. Vidare behövs också en beskrivning av det gemensamt planerade datasystemet, dess genomförande och funktion. Därtill skall avtal ingås om samarbetet och hur det skall genomföras. För projektets genomförande behövs också ett effektivt uppföljningssystem i realtid med tydlig ansvarsfördelning.

Varje verksamhetsenhet inom hälso- och sjukvården som använder sig av ett regionalt datasystem och dataförmedlingstjänster skall ingå separata uppdragsavtal med de utomstående serviceproducenterna.

Respektive verksamhetsenhet (t.ex. en hälsovårdscentral och en verksamhetsenhet för specialistsjukvård) ansvarar fortsättningsvis i egenskap av registeransvarig för sitt eget patientregister och databehandlingen i anslutning till detsamma. Serviceproducenten är ansvarig gentemot de registeransvariga på basis av avtalsansvar.

Se - SHM:s finskspråkiga avtalsmallar för hälso- och sjukvården

BILAGA 1 avtalsstruktur för uppdragsavtal

BILAGA 2 checklista med exempel på vilka/vilken typ av frågor som bör fastställas i ett uppdragsavtal

MALL FÖR ETT SKRIFTLIGT UPPDRAGSAVTAL (avtalsstruktur)

(avtalsmallen gäller i synnerhet utomstående tjänster som förutsätter personuppgiftsbehandling)

1) PARTER

* **BESTÄLLARE, (UPPDRAGSGIVARE)**

t.ex. ämbetsverket xx eller företaget xx (registeransvarig)

* **UPPDRAGSTAGARE** (t.ex. företaget xx)

- ansvar enligt avtalet

2) AVTALET GÄLLER

t.ex. tillhandahållande av databehandlingstjänster

3) UPPDRAGSGIVARENS STÄLLNING, RÄTTIGHETER OCH SKYLDIGHETER

- Uppdragsgivaren ansvarar i egenskap av registeransvarig för

* Här anges vilka funktioner i anslutning till registerföringen som hör till (kvarstår hos) uppdragsgivaren i behandlingen av personuppgifter

4) UPPDRAGSTAGARENS STÄLLNING, ÅTAGANDEN OCH SKYLDIGHETER

- Ansvar enligt uppdragsavtalet:

* Här anges vilka funktioner i anslutning till personuppgiftsbehandlingen som hör till uppdragstagaren (t.ex. ansvar för administration och skydd av databehandlingen, datasäkerhet, förvaring av uppgifter för uppdragsgivarens räkning samt tillgodoseende av rätten till insyn) (Se checklistan, bilaga 2)

- Ett omnämmande att uppdragstagaren inte har rätt att använda uppgifterna i sin egen verksamhet eller lämna ut dem

5) AVTALSSAMARBETE

- Här anges bl.a. parternas ansvarspersoner och deras uppgifter

6) PRIS

7) BETALNINGSVILLKOR

8) AVTALETS GILTIGHET

9) HÄVANDE/UPPHÖRANDE AV AVTALET

10) UPPFÖLJNING OCH TILLSYN

11) SKADESTÅND

12) AVGÖRANDE AV MENINGSSKILJAKTIGHETER OM AVTALET

13) AVTALSEXEMPLAR

14) RAPPORTERING

15) ÖVRIGA NÖDVÄNDIGA AVTALSBESTÄMMELSER

16) UNDERSKRIFTER

Se SHM:s finskspråkiga modellblanketter

FRÅGOR ATT BEAKTA NÄR UPPDRAGSAVTAL OM BEHANDLING AV PERSONUPPGIFTER UPPRÄTTAS (checklista)

Enligt 8 § 1 mom. 7 punkten i personuppgiftslagen får personuppgifter behandlas om detta behövs för betalningstjänst, databehandling eller andra därmed jämförbara funktioner som utförs på uppdrag av den registeransvarige. Nedan finns en lista på frågor/aspekter som skall beaktas vid upprättandet av uppdragsavtal.

(Listan är inte uttömmande. Avtalets innehåll beror i sista hand på vilka tjänster som skall anskaffas.)

Parter:	Har beaktats i avtalet
1. Vem är registeransvarig/uppdragsgivare? (3 § 1 mom. 4 punkten i personuppgiftslagen)	
2. Vem/vilket organ har rätt att för den registeransvarige besluta om att ge ut uppdraget?	
3. Vem är uppdragstagare? (person, sammanslutning, företag)	
4. Vem/vilket organ har rätt att ingå avtal i uppdragstagarens namn?	
5. Vilka är avtalsparternas ansvarspersoner i fråga om avtalet och vad har de för uppgifter?	
I avtalet fastställs följande:	
1. De olika faserna i personuppgiftsbehandlingen skall beskrivas och därtill skall det fastställas vilka funktioner och behandlingsfaser som omfattas av uppdragsavtalet. Vidare skall det avtalas om vilka förfaranden som skall tillämpas vid behandlingen av personuppgifter (Personuppgiftsbehandlingen kan fastställas noggrant i en tjänstebeskrivning e.d.).	
2. Uppdragsgivarens och uppdragstagarens ansvar och uppgifter skall anges specifikt för varje behandlingsfas.	
3. Bägge parter skall ha kännedom om lagarna samt myndigheternas föreskrifter och anvisningar om behandlingen av personuppgifter. Särskilt viktigt är att bestämmelser och föreskrifter om sekretess, tystnadsplikt och skydd av uppgifter beaktas.	
4. Uppdragsgivaren och uppdragstagaren sörjer för sin egen del för att bestämmelserna och myndighetsföreskrifterna om dataskydd eller övrig sekretess iakttas.	
5. Uppdragstagaren skall innan personuppgiftsbehandlingen inleds ge uppdragsgivaren tillräckliga förbindelser om att skydda personuppgifterna på det sätt som förutsätts i detta avtal. Sekretessförbindelserna skall också omfatta uppdragstagarens personal.	
6. Uppdragsgivaren är en i personuppgiftslagen avsedd registeransvarig för vars ändamål registret har inrättats och har således rätt att bestämma om dess användning. Uppdragsgivaren skall beredas möjlighet att övervaka behandlingen av personuppgifter och ge uppdragstagaren direktiv och anvisningar om behandlingen.	
7. Uppdragsgivaren och uppdragstagaren ansvarar för sin del för uppföljningen av hur personuppgifterna används. Det skall bestämmas på vilket sätt och hur ofta uppdragsgivaren skall tillställas logguppgifter och andra uppgifter som behövs för övervakningen av uppdragstagarens arbete.	
8. Uppdragsgivaren ansvarar i egenskap av registeransvarig för att de skyldigheter som nämns i personuppgiftslagen om bl.a. utarbetande och tillgänglighållande av	

en registerbeskrivning, information och tillgodoseende av rätten till insyn fullföljs. Om uppdragstagaren deltar i åtgärder som hänför sig till de registrerades rättigheter skall dessa uppgifter specificeras.	
9. Uppdragsgivaren och uppdragstagaren avtalar om datasäkerheten vid sådan behandling av personuppgifter som omfattas av uppdraget och om hur säkerhetsarrangemangen kontrolleras och uppdateras. Datasäkerhetsarrangemangen skall utvärderas med jämna mellanrum.	
10. Dataskyddet samt användarrättigheterna och datasäkerheten i anslutning till uppdragstagarens program, tillämpningar, datorer och nät som utnyttjas i de behandlingsfaser som hör till uppdraget skall specificeras och säkerställas. Uppdragsgivaren och uppdragstagaren ansvarar för sin egen del för att tekniska och organisatoriska åtgärder vidtas för att hindra att obehöriga kommer åt personuppgifterna eller att uppgifter förstörs, ändras, utlämnas eller överförs av misstag eller olagligt eller behandlas på något annat olovligt sätt.	
11. Uppdragsgivaren ansvarar för att uppdragstagaren får information om rättade, utplånade och ändrade personuppgifter. Uppdragstagaren skall beakta dessa omedelbart i den personuppgiftsbehandling som ingår i uppdraget.	
12. Uppdragsgivaren och uppdragstagaren kartlägger problemsituationerna i anslutning till utförandet av uppdraget och därtill hörande förfaringssätt och ansvar.	
13. Av avtalet skall framgå om uppdragstagaren kan anlita underleverantörer eller överföra avtalet på en tredje part. För eventuella underleverantörer gäller samma krav om dataskydd och datasäkerhet som för den egentliga uppdragstagaren. Det skall också fastställas på vilka villkor och enligt vilka förfaranden underleverantörer får anlitas.	
14. Uppdragstagaren får endast utnyttja eller lämna ut uppgifter i den omfattning som avses i avtalet och vid utförandet av en avtalsenlig uppgift. Uppdragstagaren får endast använda uppgifterna på de sätt och för de ändamål som anges i uppdragsavtalet.	
15. Uppdragstagaren förbinder sig till att personuppgifterna behandlas endast av de personer, vilkas arbetsuppgifter förutsätter detta. Uppdragsgivaren och uppdragstagaren avtalar om beviljandet av rätt att använda personuppgifter.	
16. Uppdragstagaren ansvarar för att andra kunder som eventuellt använder samma arbetsredskap inte kommer åt uppdragsgivarens uppgifter.	
17. Uppdragstagaren förbinder sig att behandla erhållna material och uppgifter som konfidentiella samt att endast använda dem för de ändamål som anges i avtalet också efter att avtalsförhållandet upphört.	
18. Uppdragstagaren skall åtgärda föråldrade personuppgifter i enlighet med de principer som har avtalats och meddela uppdragsgivaren att de har förstörts. Både tidpunkten när och det sätt på vilket föråldrat datamaterial skall förstöras skall anges. Vid förstöring av material skall lagar eller myndighetsföreskrifter om förvaring av material beaktas.	
19. Om uppdragstagaren överför avtalet eller rättigheter som hänför sig till detsamma på någon annan part, skall det avtalas under vilka förutsättningar detta kan ske.	
20. Under vilka förutsättningar kan avtalet hävas eller dess villkor ändras och hur inverkar avtalets upphörande på behandlingen av personuppgifter? Vilka åtgärder skall vidtas och vilket ansvar har parterna när uppdragsförhållandet upphör?	
21. Hur och när skall de personuppgifter som uppdragstagaren förfogar överlämnas till uppdragsgivaren/den nya uppdragstagaren eller förstöras?	
22. Hur skall fullföljandet av avtalet uppföljas och övervakas?	
23. Vilka följder och eventuella skadeståndsansvar kan ett avtalsbrott leda till och hur avgörs meningsskiljaktigheter om avtalet och den behandling av personuppgifter som avses i detsamma?	
24. Uppdragsgivaren och uppdragstagaren skall se till att dataombudsmannen	

tillställs de anmälningar som anges i personuppgiftslagen - registeransvarig som anskaffar uppdragstjänster: registeranmälan - uppdragstagare: verksamhetsanmälan	
---	--