



DATAOMBUDSMANNENS BYRÅ

PLANERING OCH FÖRVERKLIGANDE AV PORTALVERKSAMHET

Uppdaterad 14.04.2011

www.tietosuoja.fi

PLANERING OCH FÖRVERKLIGANDE AV PORTALVERKSAMHET

Anvisningens syfte

Syftet med denna anvisning är att beskriva hur kraven i personuppgiftslagen bör beaktas när portaler planeras och förverkligas. I anvisningen granskas särdragen i portalernas personuppgiftsbehandling särskilt ur synvinkeln för den registeransvariges skyldigheter. I portalerna kan förverkligas mycket olika slag av affärsverksamhetsmodeller, som leder till ett helhetsarrangemang av olika ansvar och avtal. Denna anvisning strävar till att hjälpa de registeransvariga som är verksamma i portaler att identifiera de skyldigheter som lagen uppställer samt att underlätta planeringen och förverkligandet av portalverksamheten ur dataskyddets synvinkel. I granskningen tas inte ställning till sådan kommunikation som avses i lagen om dataskydd vid elektronisk kommunikation, eller till behandlingen av identifieringsuppgifter när internet- och kommunikationsförbindelser upprättas. Också de upphovsrätts- och konsumentskyddsfrågor som är förenade med portalernas innehåll och levererandet av tjänsterna har avgränsats utanför granskningen.

Vad är en portal?

En portal har allmänt beskrivits som en kanal till av en eller flera organisationer tillhandahållna produkter, tjänster, kommunikationstjänster och informationstjänster. På internet innebär en portal således en nättjänst, som förutom sina egna funktioner kan erbjuda tillträde och ett enhetligt användargränssnitt till flera andra nättjänster. Portalen hjälper att etablera kontakter mellan olika aktörer, såsom tjänsteleverantörer och kunder.

Genom att i portalverksamheten tillse att konsumenternas integritet är tryggad och att planera och förverkliga portalverksamheten med beaktande av dataskyddet, kan företagen få en konkurrensfördel genom ett ökat förtroende. Förtroendet för de tjänster som erbjuds på internet och deras dataskydd är från konsumenternas synpunkt en av de mest kritiska förutsättningarna för att använda sig av tjänsterna.

Personuppgiftslagen och portalverksamhet

Från personuppgiftslagens synpunkt bör i portalverksamheten definieras parternas roller och ansvar samt deras åligganden vid behandlingen av personuppgifter; vem är den registeransvarige för de personuppgifter som behandlas i portalen, vilka uppgifter för olika användningsändamål inrättade personregister behandlas i portalen och hur säkerställs lagligheten för behandlingen av de personuppgifter som behandlas i portalen. Den registeransvarige (t.ex. ett företag, en myndighetsorganisation etc.) kan själv upprätthålla portalen eller den registeransvarige kan anskaffa portaltjänsterna från en utomstående tjänsteleverantör (uppdragstagare). I samma affärsverksamhetsmässiga eller tekniska portalhelhet kan behandlas uppgifter som finns i en eller flera registeransvarigas register. Om den registeransvarige anskaffar portaltjänsten från utomstående tjänsteleverantörer, uppställs för den registeransvarige särskilda krav på att säkerställa inte bara behandlingen av de personuppgifter som hör till hans egen beslutanderätt, utan också att i verksamheten tillsammans med andra registeransvarigas uppgifter inte uppkommer olagliga kombinationer av uppgifter. Då skall med på förhand begärda utredningar och avtal säkerställas, att i portalverksamheten inte t.ex. uppgifter som lämnas ut av en viss registeransvarig kombineras på ett olagligt sätt med andra registeransvarigas uppgifter.

De roller som ankommer på de registeransvariga och dem som på uppdrag behandlar personuppgifter kan identifieras t.ex. med följande enkla förfarande:

1. Identifiera vilka aktörer som i portalverksamheten behandlar **personuppgifter** och huruvida vid behandlingen uppkommer ett **personregister** (som avses i 3 § 1 momentet 3 punkten i PuppL). Ifall ett sådant uppkommer,
2. Bedöm envar aktörs roll särskilt:
 - a. Ifall den aktör som behandlar personuppgifterna är en **registeransvarig** (som avses i 3 § 1 momentet 4 punkten i PuppL), berörs denne direkt av alla krav i personuppgiftslagen.
 - b. Ifall aktören behandlar personuppgifterna på någon registeransvarigs uppdrag, baserar sig **uppdragstagarens** rätt att behandla personuppgifterna (enligt 8 § 1 momentet 7 punkten i PuppL) på ifrågavarande registeransvarigs rätt, som den registeransvariga bör kontrollera medels avtal.

Exempel:

- Portalens affärsverksamhet är helt på ett företags ansvar, men i produktionen av tjänsterna deltar företag som också behandlar personuppgifterna. Härvid är det företag som bedriver portalens affärsverksamhet den registeransvarige. Emedan ifrågavarande registeransvarige på basis av avtal anskaffar databehandlingstjänster av andra företag, som för att producera portalens tjänster också behandlar personuppgifterna, är dessa andra aktörer uppdragstagare. Uppdragstagarna behandlar personuppgifterna på basis av ett uppdragsavtal med den registeransvarige som bedriver affärsverksamheten.
- Ifall i den tjänstehelhet som utgörs av samma affärsverksamhetsmässiga och tekniska portal fungerar två eller flera leverantörer av portaltjänster (som kan vara varandra ersättande eller kompletterande produkter), men företagen fungerar som självständiga bolag och ettvarit insamlar personuppgifter enbart för sitt eget bruk, är det fråga om en s.k. situation med flera parallella registeransvariga. Då är varje företag som insamlar personuppgifter för sina egna användningsändamål en självständig registeransvarig och varje registeransvarig bör självständigt tillse att kunderna informeras om behandlingen av personuppgifterna.

Den person som använder portalen (den registrerade), t.ex. en kund hos portalen, bör få veta med vilken och vilka registeransvariga han har att göra och vem det är som utövar bestämmanderätten vid den behandling av personuppgifter som sker i portalens verksamhet. Den person som använder portalen bör i sina ärenden kunna vända sig till rätt registeransvarig. Den registeransvarig som planerar och förverkligar portaltjänster bör således planera sin registerföring och den behandling av personuppgifter som sker i den tillhörande portalverksamheten så, att han åt den registrerade kan lämna ifrågavarande uppgifter i den register- och dataskyddsbeskrivning som han har uppgjort. Denna information, som förutsätts av personuppgiftslagen, bör finnas synligt tillgänglig för användaren i samband med en tjänst som förverkligas via internet. Användaren bör således när han lämnar sina personuppgifter kunna veta, vilken registeransvarig som behandlar hans uppgifter, för vilket ändamål det sker, hur han kan utöva sina till behandlingen anknutna rättigheter samt huruvida hans uppgifter regelmässigt utlämnas

någonstans. Också informationen gällande skyddet av uppgifterna är väsentliga för den person som lämnar sina uppgifter. Ifall portaltjänsterna anskaffas från utomstående tjänsteleverantörer, är det skäl att de som är aktörer i portalen planerar informationen tillsammans.

Vad avses med en portal i dessa anvisningar?

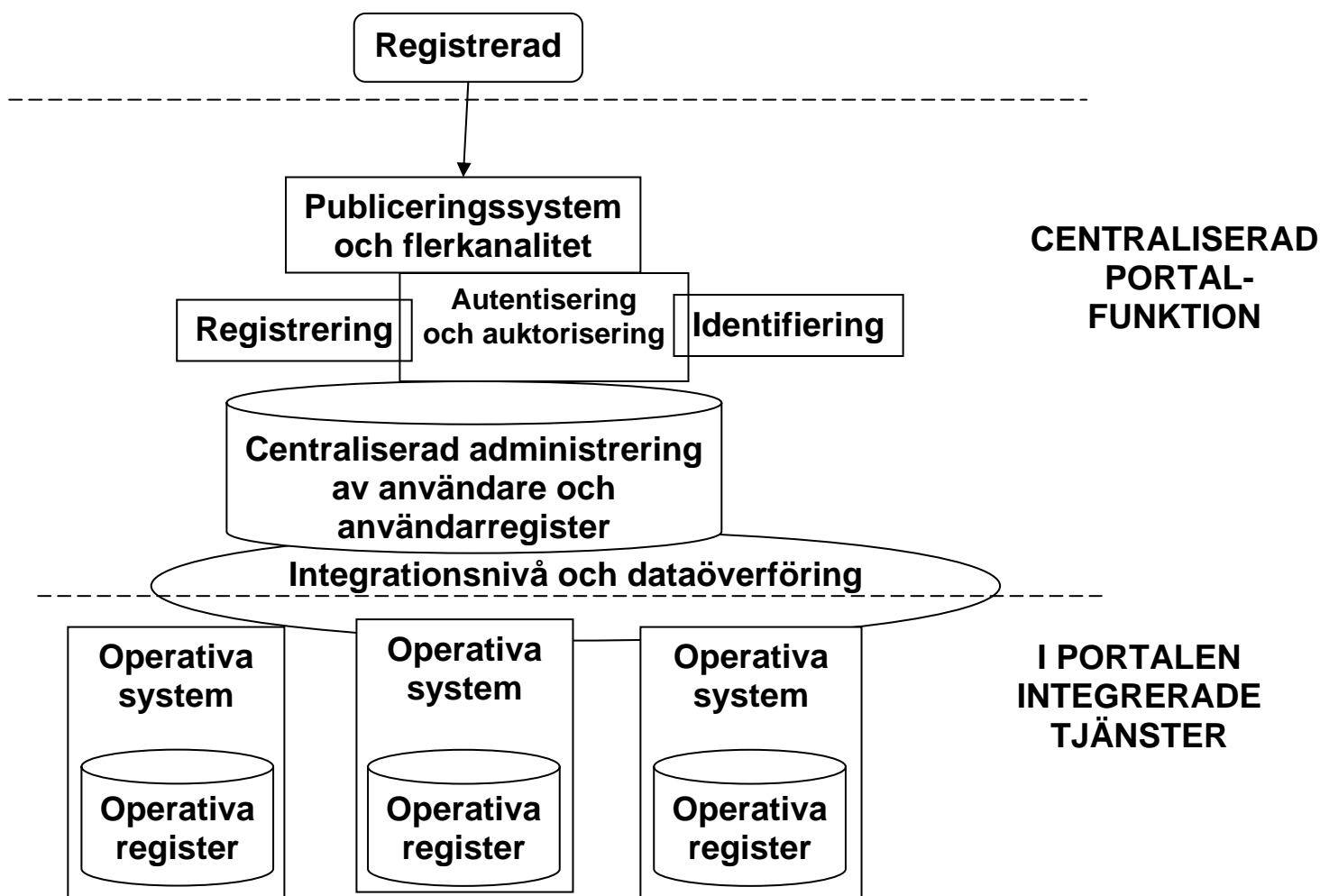
I det följande behandlas exemplifierande en elektronisk tjänstekanal som upprätthålls av ett företag (registeransvarig). Med hjälp av portalen erbjuder företaget med ett enhetligt användargränssnitt åt kunderna i en centraliserad portalstruktur integrerade tjänster som tillhandahålls av flera tjänsteleverantörer (uppdragstagare). Som exempel har använts ett företag som är verksamt inom konsumentaffärsverksamhet. Anvisningen kan emellertid i tillämpliga delar också användas när offentliga tjänster tillhandahålls. Portalen är här således företagets internet-tjänst, där konsumenten-kunden kan möta de tjänster och produkter som företaget tillhandahåller. I anvisningen granskas som exempel ett stort företags centraliserade portaltjänst, där portalens basfunktioner produceras centraliserat och de s.k. operativa tjänster som erbjuds i portalen produceras med hjälp av i portalen integrerade tjänstetillämpningar.

Den struktur hos portalen som framläggs förenklar portalens verksamhetshelhet och betonar avsiktligt de funktioner, som har direkt anknytning till behandlingen av personuppgifter. När portalens struktur granskas bör beaktas att vid småskaliga internet-tillämpningar kan hela verksamhetshelheten vara förverkligad med en enda tillämpning.

Portalverksamhetshelheten är ofta resultatet av samarbete mellan många aktörer. I samma tekniska portal kan således finnas flera aktörer, t.ex. det företag som i sin helhet svarar för portalens affärsverksamhet, företag som utvecklar och upprätthåller portalens tekniska funktion eller dess element, företag som producerar portalens olika tjänster, företag som levererar tillämpningar eller utrustningar, företag som erbjuder datakommunikationsförbindelser eller t.ex. företag som marknadsför sina produkter i portalen. Portalens tekniska förverkligande, upprätthållande och utvecklande har ofta fördelats på flera olika aktörer. I fråga om den tekniska miljön tar personuppgiftslagen inte ställning till med en hurudan teknisk miljö portalverksamheten borde förverkligas. På samma tekniska portalunderlag kan produceras flera självständiga portaler eller portalaffärsverksamheter, som alla från personuppgiftslagens synpunkt kan vara särskilda uppdragshelheter.

Centraliserade tjänster i portalen i detta förenklade exempel är internet-innehållsproduktion, tjänster för registrering, autentisering, auktorisering och identifiering av användaren samt integreringstjänster. Med systemet för internet-innehållsproduktion kan upprättas internetsidor, men eventuellt flerkanals användargränssnitt också till andra elektroniska media såsom mobiltelefoner. Registreringstjänsten erbjuder för portaltjänsten en komponent med hjälp av vilka portalens kunder kan registrera sig i portaltjänsten genom att ge uppgifter om sig själva samt acceptera nödvändiga villkor för tjänstens användning. I samband med registreringen kan kunden i allmänhet också bekanta sig med annan information som ges av tjänsteleverantören. Med autentisering, auktorisering och identifiering avses administrering av portalens användare, anknytande till identifiering av användaren, beviljande av användarrätter och specificering av användaren i portaltjänsten. Med integreringstjänster avses gränssytor och komponenter, som möjliggör att flera olika tjänstetillämpningar fungerar som delar av portalen. I produktionen av portaltjänstehelheten deltar i exemplet vid sidan av den centrala portalfunktionen flera s.k.

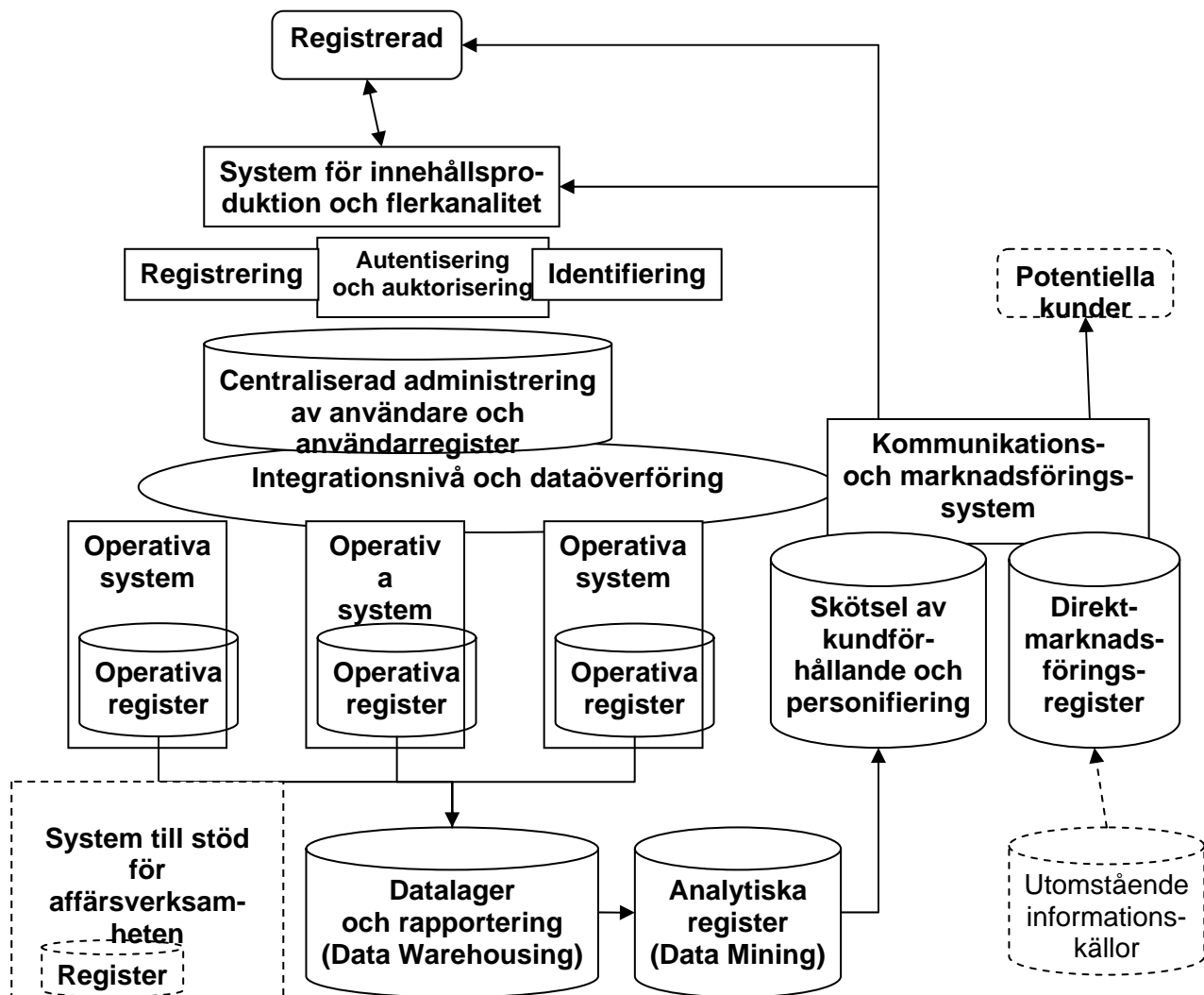
operativa tillämpningar som producerar tjänster. Med hjälp av den centraliserade portalens funktioner erbjuds användaren en annan portals operativa tjänster så, att den som använder tjänsterna inte nödvändigtvis märker skillnaden när han övergår från en tillämpning till en annan, och han upplever att han använder en enda enhetlig portal. Portalens tekniska tjänstehelhet kan sålunda utgöras av flera olika tillämpningar, som kan produceras av olika tjänsteleverantörer decentraliserat, men vilkas tjänsteutbud kan sammanföras centraliserat till ett enda portalanvändargränssnitt. Portalens centraliserade tekniska funktionella helhet har åskådliggjorts i figur 1.



Figur 1. Exempel på den centraliserade portallösningen i en registeransvarigs portal och på integrering av tjänster.

Utöver de operativa tillämpningarna kan vid företags mera omfattande portallösningar i portalen ha integrerats också system för lagring av data om kunduppgifter, analys- och marknadsföringssystem, där personuppgifter behandlas. Personuppgifter behandlas i allmänhet ofta i system till stöd för affärsverksamheten, styrning av verksamheten, fakturering och kommunikation samt i kontorstillämpningar. Ur synvinkeln för behandling av personuppgifter bör också dessa system beaktas som en del av ordnandet av dataskyddet, när med dessa behandlas personuppgifter som en del av den

registeransvariges verksamhet. En utvidgad verksamhetshelhet i portalen har åskådliggjorts i figur 2. I verksamheten bör man kunna särskilja och beskriva ändamålen för den behandling av personuppgifter som sker i olika funktioner, och det är skäl att jämföra dem med det grundläggande förhållandet mellan registeransvarig och registrerad.



Figur 2. Exempel på den utvidgade verksamhetshelheten i en registeransvarigs portal.

I en portalmiljö avses med registrerad i enlighet med 3 § 1 momentet 5 punkten i PuppL den person som en personuppgift gäller, dvs. alla användare av portalen som identifieras när de använder portalen och vilkas uppgifter behandlas när portaltjänsten förverkligas. I konsumentaffärsverksamhet är det i praktiken konsumentkunder som är registrerade. Den registeransvarige är i enlighet med 3 § 1 momentet 4 punkten i PuppL 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.

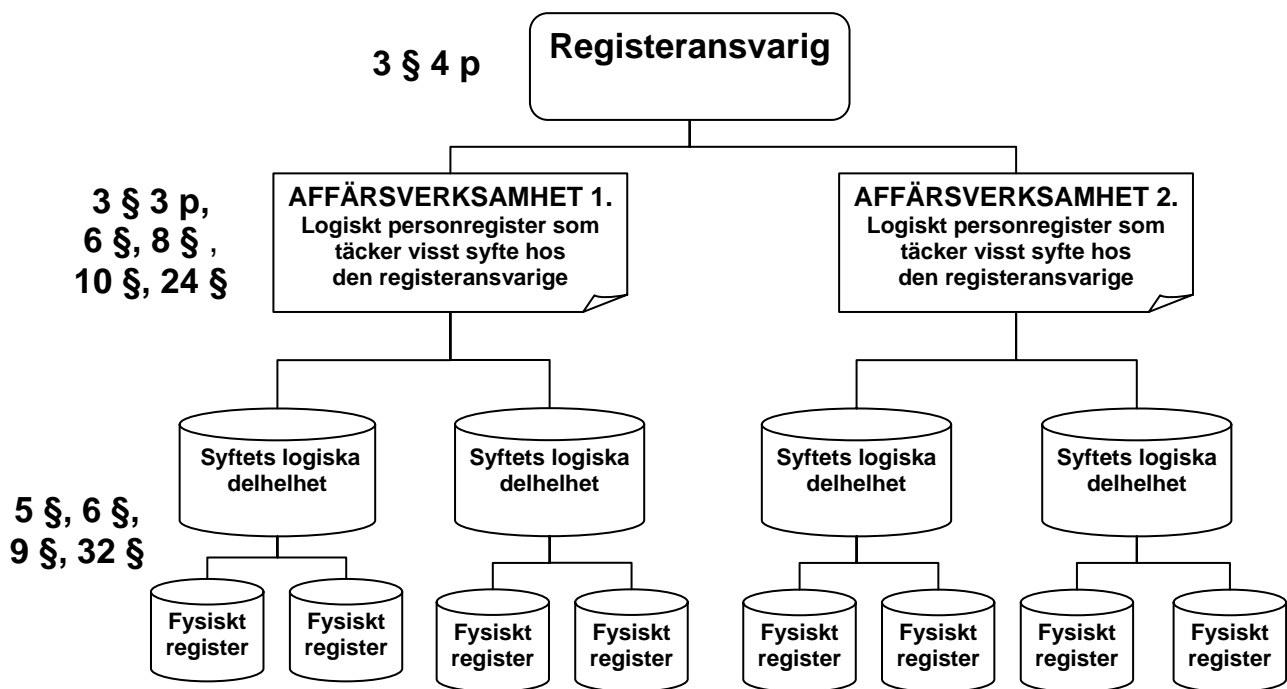
Den registeransvarig som svarar för portalens affärsverksamhet och teknologi kan anskaffa tjänster, såsom tekniskt upprätthållande av portalen, också av en utomstående tjänsteleverantör på basis av avtal. En sådan i 32 § 2 momentet i PuppL beskriven självständig näringsidkare, som handlar för den registeransvariges räkning, benämns i dessa anvisningar **uppdragstagare** och den registeransvarige på motsvarande sätt **uppdragsgivare**. När portalens tjänstehelhet utgörs av tjänster som tillhandahålls av flera olika aktörer är det särskilt viktigt att definiera och planera, vilka som svarar för behandlingen av personuppgifter som i 3 § 4 punkten i PuppL avsedd registeransvarig och vilka som behandlar personuppgifter på uppdrag i egenskap av uppdragstagare. Portalens tjänstefunktioner, affärsverksamhetsmodell och avtalsstruktur bör vara klara och kongruenta samt entydigt definierade också i fråga om rollerna vid behandlingen av personuppgifter.

Om de allmänna förutsättningarna för behandling av personuppgifter har bestämts i 8 § i PuppL. I fråga om portaler, är typiska i 8 § i PuppL avsedda allmänna förutsättningar för behandling av personuppgifter kundens dvs. den registrerades entydiga samtycke enligt 1 momentet 1 punkten och/eller den i 1 momentet 5 punkten avsedda sakliga anknytningen till den registeransvariges verksamhet, t.ex. ett kundförhållande (anknytningskravet). Också **användningsändamålen** för de personuppgifter som behandlas bör definieras i enlighet med principen för ändamålsbundenhet i PuppL 7 § så, att av dem framgår för utförandet av vilka uppgifter personuppgifterna insamlas. Användningsändamålen skall beskrivas enligt logiska helheter. Med logiskt register avses ett för ett visst syfte upprättat personregister, till vilket hör alla uppgifter som för ifrågavarande syfte insamlas och behandlas, även om uppgifterna tekniskt sett skulle förvaras i skilda register. Kravet på bundenhet till användningsändamålet i PuppL innebär, att personuppgifter som har lagrats i personregistret inte får användas för annat än det definierade användningsändamålet.

Personuppgiftslagen uppställer för den registeransvarige en **upplysningsplikt** i enlighet med 10 § och 24 § i PuppL. Registerbeskrivningen och annan erforderlig information kan i en nättjänst framläggas för den registrerade som en del av den s.k. dataskyddsbeskrivningen. I dataskyddsbeskrivningen kan man, utöver den information i registerbeskrivningen som anges i 10 § i PuppL, framlägga för den registrerade också andra uppgifter som krävs för uppfyllande av upplysningsplikten, t.ex. den information som förutsätts av 24 § i PuppL¹. Dataskyddsbeskrivningen är således ett hjälpmedel, med vilket den registeransvarige för sin del kan uppfylla den i personuppgiftslagen uppställda upplysningsplikt som är utåt synlig för den registrerade. Uppllysningsplikterna i 10 § och 24 § i PuppL hänför sig till hela syftet med behandlingen av personuppgifter såsom portalens affärsverksamhetshelhet. Informationen skall således kunna ges på syftets nivå, separat för de personregister som har upprättats för olika syften, t.ex. för att användas för ett visst ändamål i affärsverksamhet.

Upplysningar om hur upplysningsplikten uppfylls finns i dataombudsmannens byrås broschyrer "Allmän upplysningsplikt enligt personuppgiftslagen" och "Gör upp en dataskyddsbeskrivning".

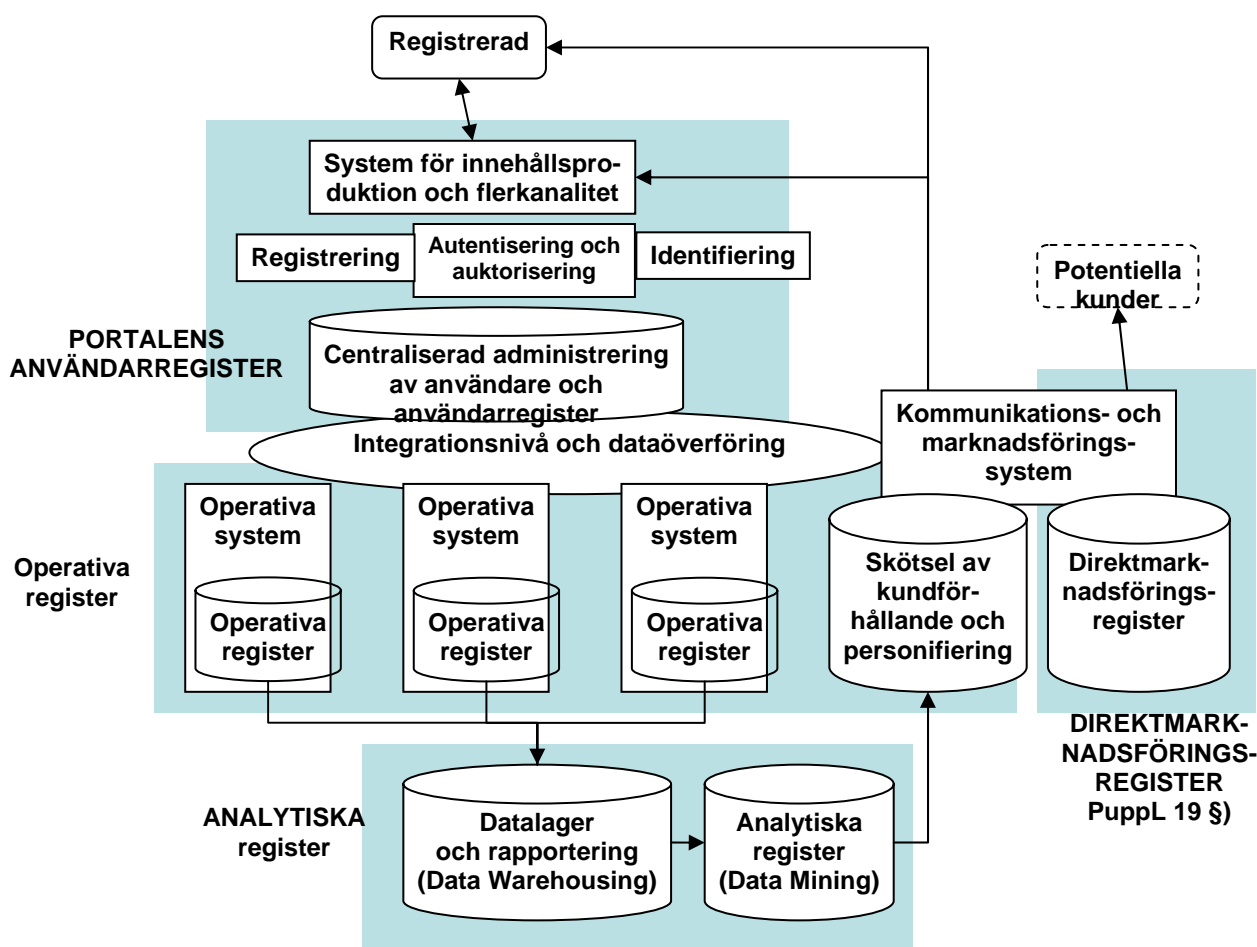
¹ Det bör också märkas, att ifall i samband med tjänsteproduktionen används cookies, bör om dessa informeras på det sätt som 7 § i lagen om dataskydd vid elektronisk kommunikation (516/2004) förutsätter.



Figur 3. Strukturen för logiska personregister.

Ett **personregister** är således i personuppgiftslagens begreppsvärld en logisk helhet. Ett personregister som har upprättats för något av den registeransvariges syften, t.ex. ett visst ändamål i affärsverksamhet, kan i mera komplicerade portalmiljöer uppdelas i flera logiska delhelheter, för att dataskyddsverksamheten skall kunna hanteras och styras. Typiska logiska delhelheter i portalmiljöer är t.ex. portalens användarregister, operativa register, analytiskt register och direktmarknadsföringsregister. Portalens användarregister är i exemplet en av de centrala portalfunktionerna och särskilt administreringen av portalens användare bildad delhelhet, i vilken behandlas personuppgifter för registrering och identifiering av användaren, administrering av användarrätter samt specificering av användaren. Det typiska användningsändamålet för delhelheten operativa register (såsom olika tillämpningar som producerar portalens tjänster, kundservice- eller kundkommunikationstillämpningar) är i portalen att producera tjänsten samt att utveckla och upprätthålla tjänsteutbudet samt att sköta, administrera och utveckla kundförhållandet. I fråga om olika operativa funktioner och tillämpningar kan också uppstå olika i personuppgiftslagen avsedda användningsändamål, som det kan vara skäl att granska som sin egen delhelhet. I den analytiska registerdelhelheten (såsom data warehousing och data mining -lösningar) förädlas och kombineras i allmänhet användaruppgifter till ny, i portalens verksamhet användbar information med ändamålet att utveckla kundförhållandet och personifiera tjänsterna och marknadsföringen. Användningsändamålen för direktmarknadsföringsregister är i allmänhet att genomföra marknadsföringskampanjer och kundrekryteringar. Systemen till stöd för affärsverksamheten eller kontorstillämpningarna har i exemplet inte presenterats särskilt, men också de måste beaktas i den funktionella helheten. Också de logguppgifter som uppkommer i datasystemen när tjänsterna används bildar eventuellt personregister i enlighet med sina olika användningsändamål. Alla dessa registerfunktioner bör planeras och beskrivas med avseende på de krav som personuppgiftslagen ställer för behandling av personuppgifter. Också behandlingarnas laglighet bör säkerställas i alla skeden av behandlingen. Med avseende på behandlingen

av personuppgifter bör alla system således beaktas som en del av ordnandet av dataskyddet, när i dem behandlas personuppgifter som en del av den registeransvariges verksamhet. De logiska delhelheternas förhållande till portalens utvidgade verksamhetshelhet åskådliggörs i figur 4.

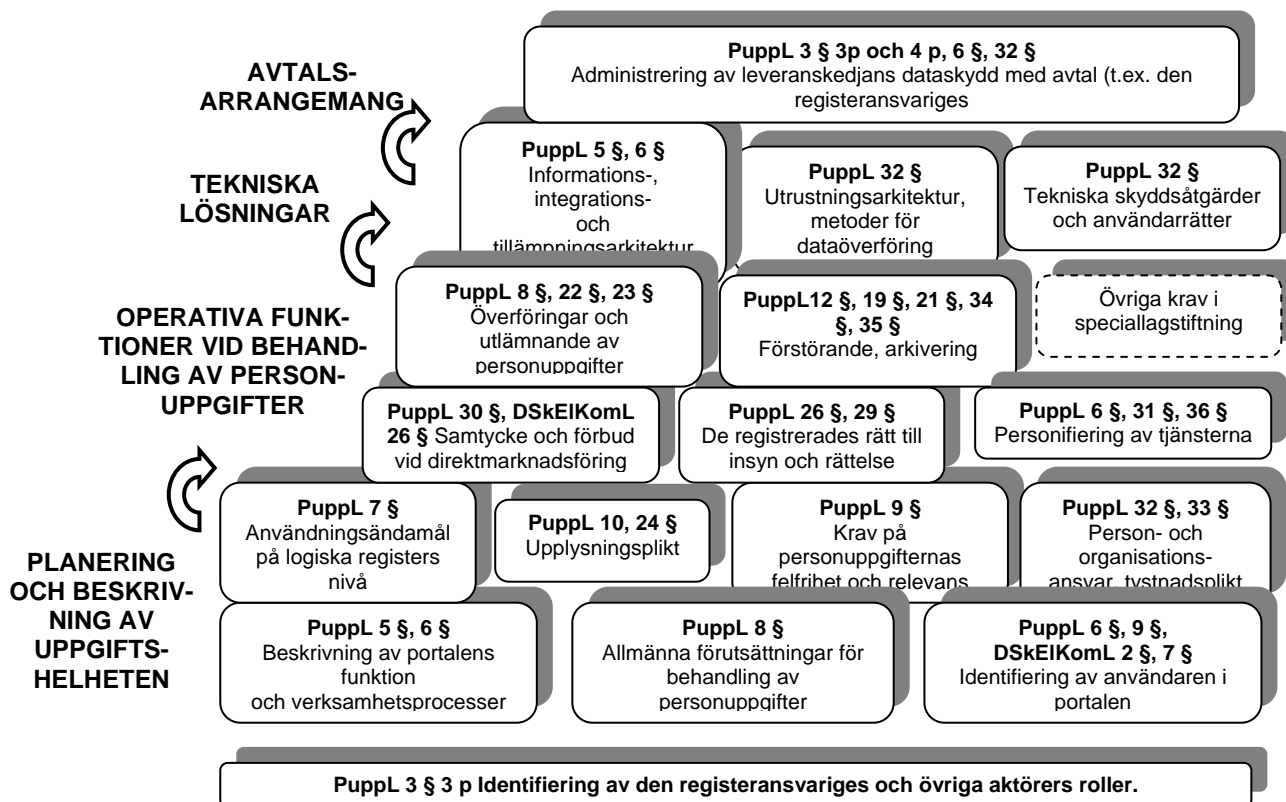


Figur 4. Exempel på logiska delhelheter i en registeransvarigs portal.

För det iakttagande av god informationshantering som anges i samband med **planeringsplikten i 6 § i PuppL och akksamhetsplikten i 5 § i PuppL** är det av nöden att försäkra sig om de funktionella förutsättningarna för behandling av portalens personuppgifter, och den registeransvarige bör analysera sin verksamhet. Eftersom vad det tekniska förverkligandet beträffar, verksamhetsprocesserna och skedena i behandlingen av personuppgifter är fast anknutna till portalens logiska arkitektur på informations-, integrations- och tillämpningsplanet, borde portalens verksamhetshelhet och verksamhetsprocesser beskrivas så i analysen, att skedena i och sätten för behandling av personuppgifter identifieras.

Planeringen av behandlingen av personuppgifter bör innefatta också den tekniska utrustningsarkitekturen, metoderna för dataöverföring samt de tekniska lösningar för dataskydd och datasäkerhet som avses i 32 § i PuppL. I planeringen och förverkligandet av portalen framskrider beaktandet av dataskyddskraven logiskt från beskrivning av

verksamheten till beskrivning av de operativa funktionerna. På basis av dessa beskrivningar kan de tekniska lösningarna planeras. Den registeransvarige skall dessutom svara för den behandling av personuppgifter som utförs av uppdragstagaren på uppdrag. Först när den registeransvariges egen verksamhet är beskriven och under kontroll, är det möjligt att ge instruktioner om och genom avtal bestämma om hur uppdragstagarna behandlar personuppgifterna. Hur planeringen och förverkligandet av portalens dataskydd framskrider åskådliggörs i figur 5.



Figur 5. Framskridningsordningen för planeringen och förverkligandet av en portals dataskydd.

Emedan de personuppgifter som gäller de registrerade är av stor betydelse för portalens upprätthållares tjänsteproduktion, är det också i den registeransvariges intresse att de skyddas. 32 § i PuppL kräver dessutom att den registeransvarige **organiserar** sin verksamhet vid behandling av personuppgifter så, att skyddet av uppgifterna blir tillgodosett. I praktiken innebär organiseringen av verksamheten en skyldighet att i organisationen utse ansvarspersoner och fördela deras ansvar och åligganden så, att man kan försäkra sig om att verksamheten som helhet är laglig och av god kvalitet. Enklast är det att göra beaktandet av dataskyddet till en så naturlig del som möjligt av organisationens normala verksamhet. Behandlingen av personuppgifter och dataskyddsverksamheten enligt den bör dokumenteras och om den bör uppgöras täckande interna instruktioner för organisationens personal. Den personal som behandlar personuppgifter, i synnerhet de som är i ansvarig ställning, bör också få en tillräcklig utbildning.

Ett särdrag i planeringen av portaltjänster är, att när portalens verksamhet planeras bör man definiera huruvida de tjänster som tillhandahålls i portalen förutsätter att **användarna**

identifieras. I fråga om olika tjänster som tillhandahålls också i samma portal är det möjligt att behoven av identifiering kan avvika från varandra. Av den som använder tjänsten bör inte krävas identifiering om inte behovet är motiverat. Den registeransvarige bör definiera nivåerna för den identifiering han tillämpar och de metoder med vilka identifieringen verkställs på olika nivåer samt gruppera de tjänster som tillhandahålls i portalen enligt identifieringsnivåerna. Det är samtidigt fråga om en planering av personuppgifternas datastruktur, som inverkar på portalens tekniska utförande. Generaliserande och förenklat kan portalens användare grupperas i fyra användargrupper på basis av nivåerna för identifieringen. Anonyma användare är på personnivån oidentifierade besökare på sidorna. De som använder pseudonymer agerar i portalen med signatur eller annan alias, utan att de i allmänhet kan förknippas med en enskild person. Svagt identifierade användare är de som har lämnat sina personuppgifter i samband med registreringen, utan att deras identitet har identifierats. Starkt identifierade är portalanvändare, vars identitet har identifierats².

Ett annat särdrag i planeringen av portaler har att göra med profileringen och personifieringen vid internet-tjänst. Med **profilering** avses här att nya uppgifter som beskriver kundens egenskaper bildas utgående från redan existerande uppgifter närmast med hjälp av analytiska datasystem. Med **personifiering** avses att dessa profiluppgifter utnyttjas för upprättandet av portalens tjänster, på så sätt att portalens användargränssnitt eller tjänster blir olika för olika kunder, så att de så väl som möjligt motsvarar deras personliga behov. Personifieringen alstras på basis av profilerna i de operativa system som producerar portalens tjänster eller i systemet för internet-innehållsproduktion. Profilering eller personifiering är inte a priori förbjudna i dataskyddslagstiftningen, men i fråga om personifiering och profilering bör den registeransvarige vara särskilt noggrann beträffande grunderna för behandlingen av personuppgifter. Om behovet av profilering och personifiering, samt särskilt om en tillräcklig felfrihet med hänsyn till profilernas användningsändamål, bör man försäkra sig på förhand i enlighet med kraven på relevans och felfrihet i personuppgiftslagens 9 §. Den registrerade skall också informeras klart i enlighet med 10 § och 24 § i PuppL om ändamålen med behandlingen av personuppgifter och om till de registrerade anknutna uppgifter eller uppgiftsgrupper som har behandlats. I fråga om personifiering bör dessutom övervägas huruvida det är fråga om ett i 31 § i PuppL avsett automatiserat beslut, när på basis av profilen portalens tjänst personifieras automatiskt och i fattandet av personifieringsbeslutet inte deltar personer och den automatiserade personifieringen har rättsliga följder för kunden eller annars kännbart påverkar honom. Om automatiserat beslut bör också i fråga om personifiering meddelas (enligt 36 § 2 momentet i PuppL) till dataombudsmannen när systemet för automatiserade beslut tas i bruk.

Det ansvar som är förknippat med den registeransvariges uppdragsgivaruppgifter omfattar vid köp av databehandlingstjänster på uppdrag utförd behandling av personuppgifter också i fråga om uppdragsgivarens verksamhet. Om de saker som är förknippade med behandlingen av personuppgifter bör avtalas skriftligt. I praktiken kan i en portalmiljö databehandlingstjänsten köpas från en utomstående genom att ett uppdragsavtal ingås mellan den registeransvarige som beställer tjänsten och den uppdragstagare som levererar tjänsten. Ifrågakavande registeransvarig ansvarar därvid för

² "Stark identifiering borde krävas vid sådana tjänster, där det behandlas konfidentiella uppgifter, såsom känsliga uppgifter enligt personuppgiftslagen eller inom organisationen sekretessbelagda uppgifter, eller när användaren kan göra sådant som är av ekonomisk eller rättslig betydelse". (Kommunikationsministeriets Luoti-publikation 8/2006 "Tietoturvaopas sähköisen palvelun tarjoajalle", s. 28 <http://www.lvm.fi/web/fi/julkaisu/view/821061> (endast på finska)

lagligheten i den behandling av personuppgifter som sker enligt uppdraget, och uppdragstagaren svarar vidare för att personuppgifterna behandlas i enlighet med det uppdragsavtal som har ingåtts mellan parterna. Emedan datasäkerhets- och dataskyddsriskerna för sin del ökar och förändras när databehandlingstjänster köps från ett utomstående företag, är det viktigt att tillräckligt i detalj definiera vilka åligganden och ansvar som kvarstår hos uppdragsgivaren. Vid uppdragen är avtalet ett verktyg med hjälp av vilket den registeransvarige kan bestämma om hur uppdragstagarna behandlar personuppgifterna, försäkra sig om dataskyddets kvalitet och hantera sina till dataskyddet anknutna risker. De omständigheter som med hänsyn till dataskyddet bör beaktas i uppdragsavtalet beskrivs i bilaga 1.

Till uppdragsavtal hörande frågor samt sätt för verkställande av den planering som saken förutsätter har också behandlats i dataombudsmannens byrås broschyr "Utkontraktering av personuppgiftsbehandling, gemensamma datasystem, samverkan i nätverk och tillhörande avtal".

BILAGA 1.

Checklista: Vad bör man avtala om i ett uppdragsavtal?

Den registeransvarige och uppdragstagaren skall avtala om den behandling av personuppgifter som är förknippad med verksamheten. Avtalets innehåll och avtalsobjektet beror från fall till fall på den tjänst som anskaffas och på den lagstiftning och praxis som är rådande på avtalsparternas bransch. I denna checklista har avsikten varit att räkna upp väsentliga på personuppgiftslagen beroende omständigheter, som i fråga om behandlingen av personuppgifter för beaktas när avtalet görs upp. I fråga om behandlingen av personuppgifter behöver inte göras upp ett separat avtal, utan det räcker att de framförda omständigheterna har beaktats i den tjänsteavtalshelhet med vilka tjänsten anskaffas. Beroende på avtalstekniken kan en del av omständigheterna i checklistan beaktas också i de i listans punkt 8 avsedda, för uppdragstagaren bindande instruktioner som ges av uppdragsgivaren. Dokumentet kompletterar de av dataombudsmannen i givna anvisningarna om ingående av uppdragsavtal och är tillämpat användbart förutom vad gäller portaler också vid behandling av personuppgifter i andra situationer av utkontraktering.

1. Parter:

- Den registeransvarige/uppdragsgivaren (PuppL 3 § 1 mom. 4 punkten) och den registeransvariges beslutsmyndiga representant.
- Uppdragstagaren och uppdragstagarens beslutsmyndiga representant.
- Parternas kontakt- och andra ansvarspersoner samt deras till behandlingen av personuppgifter anknutna åligganden.

2. Behandlingen av personuppgifter i den tjänstehelhet som anskaffas. I

tjänsteavtalet eller dess bilagor skall beskrivas skedena i behandlingen av personuppgifter, de logiska helheterna (logiska registren) skall beskrivas, och det skall definieras vilka åligganden och behandlingsskeden som omfattas av uppdraget. Det skall också beskrivas vilka verksamhets- och förfaringssätt som iakttas i behandlingen av personuppgifter. Beskrivningarna av logiska register och den logiska tillämpnings-, integrations- och informationsarkitekturen samt detaljerade beskrivningar av förfaringssätt kan fogas som bilaga till avtalet. Väsentligt är att uppdragstagarens och uppdragsgivarens ansvar och åligganden bör definieras enligt behandlingsskede med tillräcklig noggrannhet. (PuppL 5 §-6 §, 32 §)

3. Bestämmanderätt gällande kunduppgift och personuppgift. Den registeransvarige har bestämmanderätten och inom lagens ram rätt att bestämma om och behandla kunduppgifter. Denna bestämmanderätt gäller också för personuppgifter som uppkommer i uppdraget i uppdragstagarens verksamhet. Detta är utgångspunkten i personuppgiftslagen, men för undvikande av missförstånd kan det vara bra att nämna detta också i avtalet.

4. Skydd av personuppgifter och dataskydd. Uppdragstagaren skall ge uppdragsgivaren tillräckliga förbindelser om det tekniska skyddet av personuppgifterna i alla skeden av personuppgiftsbehandlingen. Med avtalsvillkor bör säkerställas att personuppgifterna skyddas mot obehörig åtkomst och mot förstöring, ändring, utlämnande och översändande som sker av misstag eller i strid med lag eller mot annan olaglig behandling. De lösningar som gäller skyddet av personuppgifter och

dataskyddet skall regelbundet utvärderas och uppdateras. Det lönar sig för den registeransvarige att i avtalet också bereda möjlighet till att anlita en utomstående auditor. (PuppL 32 §)

- 5. Sekretess.** Om sekretessbeläggning av personuppgifter och behandlingen av dem bör avtalas mellan företagen, med beaktande av också sekretessförbindelser som gäller uppdragstagarens personal. Av dem som behandlar personuppgifter kan i de mest kritiska funktionerna, såsom i fråga om känsliga uppgifter, krävas personliga sekretessförbindelser före personen godkänns för att behandla personuppgifter. De som behandlar personuppgifter bör dessutom känna till bestämmelsen om tystnadsplikt i PuppL 33 §, som gäller var och en som behandlar personuppgifter. Uppdragstagaren bör också förbinda sig till att hantera material och uppgifter som han har fått konfidentiellt samt att inte använda dem för andra ändamål enligt avtalsförhållandet. (PuppL 32 §, 33 §)
- 6. Uppföljning och tillsyn.** Den registeransvarige skall försäkra sig om sin rätt att övervaka och koordinera uppdragstagarens personuppgiftsbehandling och iakttagandet av avtalet. Den registeransvariga bör ha möjlighet att få information som är väsentlig med tanke på personuppgiftsbehandlingen. Uppdragsgivaren skall på överenskommet sätt följa med verksamheten och regelbundet rapportera om den. För uppföljning av servicenivån kan inrättas särskilda mätare för servicenivån, om vilka kan avtalas separat i ett servicenivåavtal av mera teknisk natur (SLA, Service Level Agreement) som bilaga till huvudavtalet. Likaså kan avtalas om uppföljning av verksamheten med utomstående auditeringar. (PuppL 32 §)
- 7. Dokumentation.** I avtalet skall definieras hurudan dokumentation och andra verksamhetsbeskrivningar som anknyter till dataskyddet skall upprätthållas av uppdragstagaren och på vilket sätt detta sker.
- 8. Instruktioner och föreskrifter.** Den registeransvarige bör ha möjlighet att påverka uppdragstagarens personuppgiftsbehandling under hela avtalsförhållandet samt ge instruktioner och föreskrifter angående personuppgiftsbehandlingen. (PuppL 32 §)
- 9. Överföringar av personuppgifter mellan parterna.** I avtalet skall definieras på vilket sätt, vilka uppgifter, hur ofta och under vilka villkor personuppgifter överförs mellan parterna. Också om åtkomst till och överföring av logguppgifter skall avtalas. (PuppL 8 § 2 momentet)
- 10. Utlämnning av personuppgifter till utomstående.** Uppdragstagaren får inte lämna ut personuppgifter åt utomstående annat än i den omfattning och under de förutsättningar som har definierats i avtalet. Särskilt om utlämnande av uppgifter till länder utanför Europeiska unionen bör avtalas tillräckligt i detalj. Också överföringen av personuppgifter mellan uppdragsgivarens övriga uppdragstagare som deltar i produktionen av samma verksamhet bör uppmärksammas. (PuppL 8 § 2 mom., 22 §-23 §)
- 11. Information till den registrerade.** Den registeransvarige har skyldighet att informera den registrerade. Av avtalet skall framgå, huruvida uppdragstagaren har rättigheter eller skyldigheter att bistå den registeransvarige i uppfyllandet av upplysningsplikten, t.ex. i framläggandet eller upprätthållandet av dataskyddsbeskrivningen. (PuppL 10 §,

24 §, 25 §)

- 12. Rätt till insyn, rättelse och förbud.** Det bör avtalas vilka åtgärder för tillgodoseende av den registrerades rätt till insyn, rättelse och förbud vidtas av uppdragsgivaren och vilka av uppdragstagaren. Till den del personuppgifter som skall kontrolleras eller rättas, eller förbud mot marknadsföring behandlas i uppdragstagarens informationssystem, skall man med avtal försäkra sig om att uppdragsgivarens och uppdragstagarens verksamhetsprocesser och förfaringssätt är kongruenta. Uppdragsgivaren skall svara för att behövlig information för rättande, korrigerande eller ändring av uppgifter ges åt uppdragstagaren, som har skyldighet att vidta de åtgärder som följer av informationen. I fråga om förbud mot direktmarknadsföring bör dessutom uppmärksammas administreringen av det samtycke som krävs för elektronisk direktmarknadsföring. (PuppL 26 §-28§, 29 §, 30 § och DskEIKomL 26 §)
- 13. Immateriella rättigheter, licenser och andra användarrättigheter.** Parternas rättigheter till med immateriella rättigheter skyddade objekt, t.ex. vid personuppgiftsbehandlingen behövt litterärt material eller patent, bör säkerställas. Likaså bör användarrättigheterna till vid personuppgiftsbehandlingen behövt programvara, utrustningar och dataöverföringsnät säkerställas för bägge parter. Före avtalet bör säkerställas att inte bl.a. dessa objekt graveras av tredje parts rätt eller ett avtalsvillkor, som skulle uppställa hinder för att avtala om behandlingen av personuppgifter.
- 14. Personer som behandlar personuppgifter.** I avtalet bör fastslås att personuppgifter behandlas hos uppdragstagaren endast av de personer vilkas åligganden förutsätter detta. Uppdragsgivaren och uppdragstagaren kan också avtala om ett förfarande, med vilket behandling av personuppgifter och användarrättigheter kan tilldelas, övervakas och fråntas under avtalsperioden. Det lönar sig att ägna tillräcklig uppmärksamhet åt att uppdragstagaren svarar för att personer som använder samma arbetsredskap och tillämpningar, men inte hör till dem som har godkänts på basis av avtalet, har åtkomst till uppdragsgivarens uppgifter.
- 15. Förstörande av uppgifter.** Det är bra att i avtalsvillkoren särskilt bestämma hur och när uppdragstagaren förstör föråldrade och obehövt personuppgifter och bekräftar förstörandet åt uppdragsgivaren. I avtalet skall definieras också eventuella sätt för förstörande av uppgifter och material när avtalsförhållandet upphör eller hävs. (PuppL 9 §, 32 §)
- 16. Förfarandet i problemsituationer.** Om förfarandena och ansvaren i olika slags situationer av fel, störningar och problem bör avtalas. Förfarandena bör utvärderas och uppdateras regelbundet.
- 17. Hantering av förändringar.** När verksamheten utvecklas måste också parternas verksamhet förändras. I avtalet borde definieras de mekanismer, enligt vilka parterna kan föreslå förändringar, besluta om förändringar och verkställa dem så att avtalsförpliktelse förändras i enlighet med förändringarna. Förändringarna kan också hänföra sig till tillämpningarna och den teknologi som används. Härvid borde mekanismen för hantering av förändringar vara kongruent med bl.a. förfarandena vid utvecklande av tillämpningar och systemarbete.
- 18. Uppdragstagarens användning av underleverantörer.** I avtalsvillkoren bör definieras huruvida uppdragstagaren kan, och i så fall under vilka förutsättningar,

använda underleverantörer, så att dataskyddet eller datasäkerheten inte äventyras.

- 19. Avtalets upphörande, hävande och avtalets överförande på tredje part (Exit - planer).** I avtalet bör redan i uppgörandeskedet avtalas om hur avtalets normala upphörande, hävande p.g.a. någon hävningsgrund eller avtalets överföring på tredje part inverkar på behandlingen av personuppgifter. Vilka ansvar och skyldigheter att medverka till behandlingen av personuppgifter medför åtgärden i synnerhet under övergångsskedet i behandlingen av uppgifter. De avtalsbrott som berättigar till att häva avtalet skall definieras, liksom också vad som är s.k. force majeure i fråga om informationssystem och dataskydd. Det bör även avtalas om hur personuppgifterna överförs till den nya part som skall behandla personuppgifterna eller hur de förstörs. I avtalet bör definieras huruvida uppdragstagaren får överföra avtalet vidare och under vilka förutsättningar.
- 20. Skadeståndsansvar och avtalsvite.** Om uppdragstagarens skadeståndsskyldighet samt om dess grunder bör avtalas. Om skadeståndsansvarets omfattning bör i avtalet intas en klausul i synnerhet i fråga om direkta skador. För avtalsbrott kan också direkt påföras avtalsvite. Särskild uppmärksamhet bör ägnas åt att definiera hurudan en sådan dataskyddsförbrytelse är som utlöser skadestånd eller i fråga om dataskyddet avtalsvite, och vad som i fråga om informationssystem och dataskydd utgör s.k. force majeure. (PuppL 47 §)
- 21. Lösande av meningsskiljaktigheter mellan parterna.** Parterna kan i avtalet fastslå förfarandena vid lösande av meningsskiljaktigheter mellan parterna då det gäller meningsskiljaktigheter angående behandlingen av personuppgifter.
- 22. Val av forum och val av lag som tillämpas.** De lönar sig att i avtalet definiera vilken den behöriga domstolen är, samt vilka lagar eller vilken ramlagstiftning som i fråga om behandlingen av personuppgifter skall tillämpas också med hänsyn till dataskyddet. I stället för domstol kan man också avtala om att meningsskiljaktigheter skall lösas med skiljemannaförfarande.
- 23. Kännedomen om dataskyddslagstiftningen.** När avtalet görs upp bör man försäkra sig om och dokumentera att de lagar samt föreskrifter och instruktioner av myndigheterna som gäller behandling av personuppgifter är kända av bägge parter. (PuppL 32 §)