Rollfördelning för korrekt personuppgiftsansvar

– enligt dataskyddsreglerna

Mars 2019

SVENSKT NÄRINGSLIV

Författare: Martin Brinnen och Mikael Bock, advokatfirman Kahn Pedersen

Förord

Sedan dataskyddsförordningen, GDPR, trädde i kraft har många företag pekat på svårigheter att reda ut vem som är personuppgiftsansvarig för personuppgiftsbehandlingar. Kartläggning av ansvarsfördelningen behöver göras för alla situationer då personuppgifter lämnas ut, inte minst i upphandlingssammanhang. Med de nya reglerna på plats är det viktigt att veta vem som är personuppgiftsansvarig och personuppgiftsbiträde innan anbudsförfarandet kan inledas. I en och samma upphandling kan parterna ha flera roller. Den beställande parten kan vara personuppgiftsansvarig för utlämnandet av personuppgifter. Företaget som tar emot personuppgifterna kan bli personuppgiftsbiträde för viss behandling men också självständig eller gemensamt personuppgiftsansvarig för vidare behandling av mottagna personuppgifter.

Syftet med den här skriften är att ge en vägledning till företag för att motverka att avtal sluts med stöd av felaktiga bedömningar om personuppgiftsansvaret. I skriften redovisas en metod för att systematiskt göra bedömningar av personuppgiftsansvaret vid komplexa behandlingssituationer där flera aktörer behandlar personuppgifter.

Den här skriften adresserar de aktuella frågeställningarna utifrån bestämmelserna i dataskyddsförordningen[1] och den svenska lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) (gemensamt ”Dataskyddslagstiftningen”).

Martin Brinnen och Mikael Bock, advokatfirman Kahn Pedersen, har på uppdrag av Svenskt Näringsliv tagit fram denna skrift om hur personuppgiftsansvaret ska fördelas.

Stockholm mars 2019

Carolina Brånby, jurist digital policy och Birgitta Laurent, jurist och upphandlingsexpert,
Svenskt Näringsliv

1 Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Innehåll

1. Sammanfattning 6

2. Kartlägg behandlingen av personuppgifter 8

2.1 Kartlägg behandlingen 8

2.2 Ändamål – särskilda, uttryckligt angivna och berättigade 8

2.3 Beskriv hur personuppgifterna hanteras – flödet 9

2.4 Typ av personuppgifter och kategorier av registrerade 9

2.5 IT-system med mera 10

3. Bedöm och fastställ personuppgiftsansvaret 11

3.1 Personuppgiftsansvarig 11

3.2 Gemensamt personuppgiftsansvariga 16

3.3 Personuppgiftsbiträde 19

3.4 Behandling av anställda och medhjälpares uppgifter 22

3.5 När kommuner anlitar privata utförare och entreprenörer 23

4. Reglera och dokumentera förhållandet mellan aktörerna 27

4.1 Oftast ett krav att reglera ansvaret 27

4.2 Avtal för utlämnande till självständig personuppgiftsansvarig 27

4.3 Inbördes arrangemang för gemensamt personuppgiftsansvar 28

4.4 Biträdesavtal och avtal med underbiträden 28

4.5 Instruktioner till medhjälpare 29

5. Checklistor för personuppgiftsansvar 30

5.1 Kartlägg behandlingen eller behandlingarna 30

5.2 Fastställ personuppgiftsansvaret 31

1. Sammanfattning

Dataskyddsförordningen har två syften. Den fastställer bestämmelser för att skydda personers grundläggande fri- och rättigheter vid personuppgiftsbehandling och det fria flödet av dessa uppgifter inom unionen, artikel 1 dataskyddsförordningen. Huvudansvaret för att tillse att detta skydd skapas och upprätthålls ligger på den personuppgiftsansvarige eller de personuppgiftsansvariga som har ett gemensamt personuppgiftsansvar. Ett begränsat ansvar kan också bäras av ett personuppgiftsbiträde om den personuppgiftsansvarige väljer att anlita sådant biträde. Anställda och andra fysiska personer som utför arbete under en personuppgiftsansvarigs eller ett personuppgiftsbiträdes överinseende brukar betecknas som medhjälpare. Dessa bär normalt inget ansvar för personuppgiftsbehandling som de utför åt sin arbetsgivare eller uppdragsgivare.

När flera av dessa aktörer är inblandade i en och samma behandling av personuppgifter finns det behov av att fastställa och reglera ansvaret mellan aktörerna. I det stora flertalet fall är det relativt uppenbart hur detta ska göras.

I mer komplicerade behandlingssituationer är det dock lämpligt att gå systematiskt tillväga för att få en korrekt bedömning av fördelning av personuppgiftsansvaret. Vi rekommenderar därför att man använder en arbetsmetod som beskrivs nedan men vill samtidigt påpeka att det i vissa fall går att hitta stöd för flera olika lösningar. Det är i sådana fall viktigt att kunna motivera den lösning som man väljer och att dokumentera sin bedömning.

Personuppgiftsansvar utgår från den som bestämmer över behandlingen. Det är därför nödvändigt att inledningsvis kartlägga den aktuella behandlingen eller behandlingarna. Först efter en sådan kartläggning är det möjligt att bedöma och fastställa personuppgiftsansvaret för respektive behandling.

Oavsett hur personuppgiftsansvaret sedan fördelas är det viktigt att fördelningen av ansvaret klargörs mellan de inblandade aktörerna. Det görs vanligen genom olika former av avtal och instruktioner. Vid biträdessituationer kallas avtalen för personuppgiftsbiträdesavtal eller bara biträdesavtal och är ett krav enligt dataskyddsförordningen. I andra sammanhang kallas de vanligen för datadelningsavtal (vilket kan innefatta biträdesavtal).

En arbetsmetod för bedömning av personuppgiftsansvaret vid mera komplicerade behandlingssituationer kan således sammanfattas i följande tre steg.

1. Kartlägg personuppgiftsbehandlingen (avsnitt 2)

2. Fastställ ansvarsfördelningen till något av följande alternativ (avsnitt 3)

   a. överföring mellan självständiga personuppgiftsansvariga,

   b. behandling av flera gemensamt personuppgiftsansvariga,

   c. behandling med hjälp av personuppgiftsbiträde eller

   d. behandling med hjälp av medhjälpare.

3. Reglera och dokumentera förhållandet mellan inblandade aktörer (avsnitt 4)

   a. Om självständiga personuppgiftsansvariga – överväg om datadelningsavtal ska upprättas mellan de personuppgiftsansvariga.

   b. Om gemensamt personuppgiftsansvariga – reglera i datadelningsavtal.

   c. Om personuppgiftsbiträde – reglera i personuppgiftsbiträdesavtal.

   d. Om behandling med hjälp av medhjälpare – instruktioner för behandlingen ska meddelas.

2. Kartlägg behandlingen av personuppgifter

2.1 Kartlägg behandlingen

Personuppgiftsansvaret definieras inte för en viss verksamhet, uppdrag eller liknande. Avgörande är i stället vad som utgör behandlingen, det vill säga behandlingen av personuppgifter. Inledningsvis måste därför den aktuella personuppgiftsbehandlingen identifieras och avgränsas.

Definitionen i artikel 4.2 dataskyddsförordningen av vad som utgör en behandling är mycket vid.

> *”[B]ehandling: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.”*

Definitionen ger begränsad vägledning för att identifiera vad som skiljer en behandling från en annan. Utgångspunkt för denna bedömning måste tas i ändamålen med behandlingen, det vill säga skälet för att personuppgifter behandlas. I bedömningen måste dock även hänsyn tas till många andra faktorer såsom vilka kategorier av personuppgifter som behandlingen omfattar, hur de samlas in och behandlas, vilka aktörer som behandlar personuppgifterna och hur de lämnas vidare.

En kartläggning av behandlingen fyller inte bara funktionen att utgöra ett underlag för klargörande av personuppgiftsansvaret. Den är också nödvändig för att uppfylla skyldigheten att föra en förteckning över behandlingarna, enligt artikel 30 dataskyddsförordningen, och för att informera de registrerade vid insamlingen av personuppgifter och vid begäran om registerutdrag. Notera att både i sådan förteckning och i information till de registrerade ska det framgå vem eller vilka som är personuppgiftsansvarig(a).

2.2 Ändamål – särskilda, uttryckligt angivna och berättigade

Ändamålen med en viss personuppgiftsbehandling är avgörande för bedömningen av om behandlingen är laglig. Ändamålen har även avgörande betydelse för att fastställa vad som utgör en behandling och därmed även för vem eller vilka som är personuppgiftsansvarig(a).

Personuppgifter får endast behandlas för särskilda, uttryckligt angivna och berättigade ändamål, artikel 5.1 b dataskyddsförordningen. Att ändamålen ska vara särskilda innebär att beskrivningen av ändamålen måste vara relativt detaljerad. I princip ska man av beskrivningen kunna förstå hur personuppgifterna kommer att behandlas. Det är en förutsättning för att kunna bedöma om behandlingen sker i överensstämmelse med dataskyddsförordningen.

Tänk på att ett ändamål kan vara helt eller delvis gemensamt för flera inblandade aktörer. Om behandlingen omfattar flera ändamål som är närliggande kan det vara lämpligt att beskriva dem både med en generell beskrivning till exempel lönehantering som sedan kompletteras med specifika ändamål såsom utbetalning av lön, sammanställning av lönestatistik för löneförhandlingar, överföring av obligatoriska uppgifter till Skatteverket.

Att ändamålen ska vara ”uttryckligen angivna” innebär bland annat att det inte får finnas några underförstådda eller oklara ändamål. Det ska vara klart för alla inblandade – de som ska behandla personuppgifter, de registrerade, tillsynsmyndigheter med flera – vad ändamålen innebär.[2]

2.3 Beskriv hur personuppgifterna hanteras – flödet

Hur uppgifterna samlas in, vilka som har tillgång till dem, hur de lämnas ut och när de raderas har vanligtvis stor betydelse för att förstå hur personuppgiftsansvaret fördelas. Det gäller särskilt om personuppgifter samlas in från någon annan än den registrerade, om uppgifterna behandlas av andra än anställda och om uppgifterna lämnas ut till någon utanför organisationen till exempel till ett personuppgiftsbiträde. Om uppgifterna används både av den egna organisationen och utomstående till exempel genom ett omfattande uppgiftsutbyte eller genom användning av ett gemensamt system har det betydelse för bedömning av personuppgiftsansvaret. Tillgången till ett system – i egen drift eller i en gemensam molntjänst – kan antingen vara ett utlämnande eller en behandling som utförs gemensamt.

Det är därför lämpligt att noga beskriva personuppgifternas flöde, om inte det redan har gjorts.

2.4 Typ av personuppgifter och kategorier av registrerade

Med typ av personuppgifter avses en generell beskrivning av vilka personuppgifter som ska behandlas, till exempel kontaktuppgifter, adressuppgifter och lön. Därutöver bör även anges om särskilda kategorier av personuppgifter kommer att behandlas, det vill säga känsliga personuppgifter enligt artikel 9 dataskyddsförordningen, uppgifter om lagöverträdelser enligt artikel 10 dataskyddsförordningen, person- och samordningsnummer (se artikel 87 dataskyddsförordningen och 3 kap. 10 § dataskyddslagen). Även andra typer av integritetskänsliga

2 Se Artikel 29-gruppens Opinion 03/2013 on the purpose limitation. WP 203, s. 17.

personuppgifter bör anges, särskilt sådana som kan omfattas av sekretess enligt offentlighets- och sekretesslagen, till exempel uppgifter om en persons privatekonomi, uppgifter om sociala förhållanden och värderande uppgifter till exempel från utvecklingssamtal.

Kategorier av registrerade, till exempel anställda och skolelever, är en viktig del av beskrivningen av personuppgiftsbehandlingen.

2.5 IT-system med mera

Vilka IT-system som används bör anges och beskrivas för att underlätta fastställandet av personuppgiftsansvaret. Observera dock att de tekniska detaljerna oftast är av mindre intresse för att avgöra personuppgiftsansvaret. Observera även att beslut om medel såsom vilka IT-system som ska användas kan delegeras till ett personuppgiftsbiträde. Som nämnts ovan, kan dock aldrig beslut om ändamålet delegeras.

3. Bedöm och fastställ personuppgiftsansvaret

3.1 Personuppgiftsansvarig

3.1.1 Bestämmanderätt

Personuppgiftsansvarig (controller) är den eller de som bestämmer varför och hur personuppgifter ska behandlas. Enligt den fullständiga definitionen i artikel 4.7 dataskyddsförordningen är personuppgiftsansvarig:

> *”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.”*

Personuppgiftsansvarig kan således vara en fysisk person men är nästan alltid en juridisk person; en statlig myndighet, en kommunal nämnd, ett moderbolag eller ett dotterbolag i en koncern. Det är således normalt inte en chef, en anställd, en styrelseledamot eller liknande som är personuppgiftsansvarig.

Enligt definitionen har den personuppgiftsansvarige bestämmanderätt över ändamålen och medlen för behandlingen i fråga men har möjlighet att delegera beslut om medlen. Med rätten att bestämma över ändamål och medel avses rätten att bestämma över ”varför” respektive ”hur” en behandling ska utföras.

Ändamål och medel för en behandling kan, såsom framgår av definitionen, fastställas i nationell rätt eller unionsrätt. I sådana fall kan personuppgiftsansvaret direkt eller indirekt framgå av denna reglering (uttrycklig behörighet). Ett exempel på när personuppgiftsansvaret fastställs på detta sätt är personuppgiftsansvaret för socialnämnder (se förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten).

Behörigheten att bestämma över behandlingen kan också vara underförstådd (eller presumerad) till exempel att arbetsgivare är personuppgiftsansvarig när denna behandlar personuppgifter om sina anställda eller när en förening behandlar personuppgifter om sina medlemmar (underförstådd behörighet).

Vanligast är dock att personuppgiftsansvaret grundas på faktiskt inflytande över ändamålen med och medlen för behandlingen.[3]

3 Begreppen rättslig behörighet, underförstådd behörighet och behörighet genom faktiskt inflytande härrör från Artikel 29-gruppens yttrande 1/2010 om begreppet registeransvarig och registerförare, WP 169.

3.1.2 Den som faktisk bestämmer

Det faktiska inflytandet bedöms utifrån de faktiska omständigheterna som kan framgå av bland annat avtal mellan de inblandade aktörerna eller av vem som i praktiken har avgörande inflytande.

EXEMPEL: **INKÖP AV KOMMUNIKATIONSTJÄNST**

När en aktör använder sig av kommunikationstjänster och översänder information som innehåller personuppgifter med hjälp av dessa tjänster blir aktören personuppgiftsansvarig för personuppgiftsbehandlingen som består av överföringen. Leverantören av tjänsterna blir självständigt personuppgiftsansvarig för den behandling som sker genom fakturering och trafikövervakning men inte för den behandling som överföringen utgör.[4]

3.1.3 Stort "manöverutrymme" tyder på personuppgiftsansvar

Den som har stort manöverutrymme att själv välja när, varför och hur personuppgifter ska behandlas för att kunna leverera en tjänst till en annan aktör eller för att fullgöra ett uppdrag för denne, har normalt ett personuppgiftsansvar, antingen som ensam personuppgiftsansvarig eller som gemensamt personuppgiftsansvarig. Ett stort manöverutrymme innebär att aktören själv kan bestämma över ändamål och medel för behandlingen. Det är vanligen fallet när behandlingen av personuppgifter inte är det huvudsakliga föremålet för det arbete som leverantören utför för att kunna leverera tjänsten eller fullgöra uppdraget. Som exempel kan nämnas ett företag som bedriver skolverksamhet på uppdrag av en kommun eller en transportör som ska leverera varor till slutkund enligt avtal med en e-handlare. I dessa fall är avtalsförpliktelsen som ska uppfyllas skolverksamhet respektive transport. För att uppfylla avtalsförpliktelsen kan företaget vara tvunget att behandla personuppgifter men har dock friheten att själv välja om, hur och när behandlingen ska utföras.

4 Jfr skäl 47 dataskyddsdirektivet och exempel 1 i Artikel 29-gruppens yttrande 1/2010 om begreppet registeransvarig och registerförare, WP 169.

EXEMPEL: **UPPHANDLAT ÄLDREBOENDE**

En kommun har i sitt underlag för upphandling av utförare av äldreboenden ställt som krav att ett personuppgiftsbiträdesavtal ska tecknas med kommunen. Ett företag som avser att lämna ett anbud ifrågasätter om den som driver ett äldreboende ska anses vara personuppgiftsbiträde.

Ett företag som bedriver äldreboende behandlar normalt personuppgifter om de boende för egna ändamål bland annat för att kunna ge service och vård och för att uppfylla rättsliga skyldigheter som åligger utföraren. Det huvudsakliga ändamålet med avtalet med kommunen är inte att behandla personuppgifter. Företaget utför sina uppgifter under eget ansvar och har relativt stort manöverutrymme att bestämma hur personuppgifterna ska behandlas. Kommunens möjligheter att utfärda instruktioner för personuppgiftsbehandlingen kan begränsas av speciallagstiftning som gäller för företagets verksamhet och inför vilken företaget bär ett eget självständigt ansvar. Dessa omständigheter talar för att företaget har ett eget personuppgiftsansvar. Undantag kan dock behöva göras i de fall det sker ett regelbundet informationsutbyte med kommunen till exempel för återrapportering, uppföljning och hantering av klagomål från de boende.

Bedömning av personuppgiftsansvaret kan bli komplicerat om den som normalt utför arbete under ett eget självständigt personuppgiftsansvar mottar detaljerade instruktioner från en uppdragsgivare. Det gäller särskilt om uppdragsgivaren även tillhandahåller personuppgifterna som kan behandlas för uppdragets utförande. Ett exempel är ett konsultföretag som får i uppdrag att analysera och ta fram en rapport utifrån personuppgifter som tillhandahålls av uppdragsgivaren. I dessa fall kan det vara lämpligast att betrakta båda aktörerna som gemensamt personuppgiftsansvariga.

3.1.4 Avtal mellan aktörerna

De inblandade aktörernas egna uppfattningar om ansvarsfördelning har betydelse men är inte ensamt avgörande. De inblandade aktörerna kan därför inte helt fritt styra över hur personuppgiftsansvaret ska fördelas. Ett avtal kan ge viss vägledning om hur parterna har uppfattat personuppgiftsansvaret så länge som avtalet återspeglar de faktiska omständigheterna. Men även de registrerades uppfattning om personuppgiftsansvaret och deras rimliga förväntningar har betydelse för bedömningen. Det sagda innebär att en part, kanske utifrån en maktposition, inte kan påtvinga andra aktörer sin uppfattning av hur personuppgiftsansvaret ska fördelas. Det krävs i mer komplicerade fall en mer noggrann bedömning och att samtliga parter är överens. Ytterst kan frågan avgöras av tillsynsmyndigheten eller av domstol.

Den personuppgiftsansvariges synlighet gentemot de registrerade samt de registrerades förväntningar till följd av detta kan, som nämnts ovan, ha betydelse för bedömningen.

EXEMPEL: **UTLAGD KUNDTJÄNST**

En aktör lägger ut sin kundtjänst på entreprenad och instruerar entreprenören hur dennes anställde ska presentera sig vid kontakt med kunderna. De som ringer till kundtjänsten får information om att de har ringt till aktören. I det här fallet leder uppringande personernas förväntningar och det sätt som den personuppgiftsansvarige presenterar sig för dem via telefon till slutsatsen att entreprenören agerar som personuppgiftsbiträde för kommunen.[5]

3.1.5 Personuppgiftsansvarig kan delegera vissa beslut

Genom avtal kan den personuppgiftsansvarige delegera beslutanderätten över medlen för behandlingen, i vart fall vad avser tekniska och organisatoriska frågor, som till exempel vilka IT-system som ska användas. Personuppgiftsansvarig kan även delegera frågor som normalt beslutas av denne, såsom vilka uppgifter som ska behandlas, hur länge de ska behandlas, och vem som får tillgång till dem. Beslutanderätten över ändamålen kan dock aldrig delegeras. Bestämmanderätten kan dock i vissa fall bli mer fiktiv än verklig, till exempel när ett mindre företag ansluter sig till en tjänst som tillhandahålls enligt standardiserade villkor av en myndighet eller ett globalt företag. Beslutanderätten består i dessa fall av att godkänna villkoren eller att avstå från att använda tjänsten (take-it-or-leave-it).

3.1.6 Den som har ett uppdrag eller skyldighet enligt lag

Den som har ett uppdrag eller en skyldighet enligt lag eller annan författning att samla in, publicera, tillhandahålla, bevara eller på annat sätt behandla vissa personuppgifter är vanligtvis personuppgiftsansvarig för den behandling som är nödvändig för utförandet av uppdraget eller fullgörandet av skyldigheten. Det gäller även om denne inte är formellt utpekad i författningen som personuppgiftsansvarig (jämför med uttrycklig behörighet under rubrik 3.1.1).

3.1.7 Det huvudsakliga ändamålet med avtalet

När en aktör anlitar en annan aktör för utförande av en tjänst är det viktigt att identifiera vad som utgör leverantörens huvudsakliga prestation enligt avtalet. Om den huvudsakliga prestationen enligt avtalet är behandling av personuppgifter är leverantören vanligtvis ett personuppgiftsbiträde när denne behandlar personuppgifter för den personuppgiftsansvariges räkning. Om den huvudsakliga prestationen enligt avtalet däremot är något annat än behandling av personuppgifter, till exempel hantverkstjänster, har oftast leverantören ett eget självständigt personuppgiftsansvar och situationen innebär ett utlämnande av personuppgifter från en självständig personuppgiftsansvarig (den part som anlitar hantverkaren) till en annan (hantverkaren). I dessa fall spelar tjänsteleverantörens traditionella roll och yrkeskunnande vanligtvis en framträdande roll vid genomförandet av tjänsten.

5 Jfr exempel 20 i Artikel 29-gruppens yttrande 1/2010 om begreppet registeransvarig och registerförare, WP 169.

EXEMPEL: **ANLITANDE AV ADVOKAT**

En aktör anlitar en advokatfirma för att företräda aktören i domstol vid ett överklagande av ett upphandlingsbeslut. Den behandling av personuppgifter som är nödvändig för utförandet av uppdraget utförs utan närmare instruktioner från aktören och utgör en biprodukt av uppdraget. Uppdraget består av att företräda klienten i domstol, vilket är en verksamhet som jurister traditionellt har sin egen rättsliga grund för. Advokatfirman måste därför anses bära ett eget självständigt personuppgiftsansvar för den nödvändiga personuppgiftsbehandlingen. Aktören är personuppgiftsansvarig för det eventuella utlämnande av personuppgifter som de gör till advokatfirman.[6]

3.1.8 Författningsreglerad verksamhet

Verksamheter som kringgärdas av författningsreglering eller andra regler som begränsar verksamheternas möjligheter att ta emot instruktioner från utomstående om hur personuppgifter ska behandlas till exempel på grund av tystnadsplikt, etiska regler, regler om anmälningsskyldighet bär normalt ett eget personuppgiftsansvar. Som exempel kan nämnas bank- och finansverksamhet, advokat- och revisorsverksamhet. En prövning måste dock göras i det enskilda fallet eftersom det är möjligt att dessa aktörer, beträffande vissa behandlingar, har möjlighet att ta emot instruktioner avseende personuppgiftsbehandling och samtidigt uppfylla sina regulatoriska skyldigheter.

3.1.9 Tillgång till personuppgifterna

Att den personuppgiftsansvarige bestämmer över ändamål och medel behöver inte innebära att denne faktiskt utför behandlingen eller har tillgång till personuppgifterna. Normalt har den personuppgiftsansvarige tillgång till personuppgifterna som behandlas men det är inte en förutsättning i vart fall inte när det avser ett gemensamt personuppgiftsansvar.

I målet C-25/17, Jehovas vittnen,[7] ansåg EU-domstolen att en församling var gemensamt personuppgiftsansvariga med sina medlemmar och att det för detta ansvar inte krävdes att de hade tillgång till personuppgifterna. Det var tillräckligt att samfundet organiserade, samordnade och uppmuntrade den predikoverksamhet som medlemmarna ägnade sig åt.

Högsta förvaltningsdomstolen har ansett att avsaknaden av faktisk möjlighet att påverka hur personuppgifterna hanteras innan de blir tillgängliga för den personuppgiftsansvarige inte hindrar att denne åläggs att redovisa säkerheten för en anvisad kommunikationskanal. Det kan dock medföra svårigheter vid

6 Jfr exempel 21 i Artikel 29-gruppens yttrande 1/2010 om begreppet registeransvarig och registerförare, WP 169.

7 Mål C-25/17, Jehovas vittnen, ECLI:EU:C:2018:551.

bedömningen av de skyldigheter och sanktionsmöjligheter som föreskrivs i personuppgiftslagen (1998:204) (”PUL”) och som tar sikte på personuppgiftsansvaret. Frågan i målet gällde om Försäkringskassan på grund av sitt personuppgiftsansvar hade skyldighet att utföra en risk- och sårbarhetsanalys för ett kommunikationssätt (sms) som anvisades av Försäkringskassan.[8]

3.1.10 I tveksamma fall – det alternativ som ger bäst skydd för de registrerade

I fall där det är tveksamt vem eller vilka som ska bära ett personuppgiftsansvar bör man utgå från dataskyddsförordningens syfte att skydda de registrerades friheter och rättigheter. Den lösning som ger det bästa skyddet för de registrerades personuppgifter ska väljas, artikel 1.2 dataskyddsförordningen. Det kan innebära att den aktör som har störst möjlighet att påverka behandlingen, till exempel att utföra en rättelse eller radering, anses ha ett personuppgiftsansvar. De registrerades uppfattning om personuppgiftsansvaret kan, som nämnts ovan, också ha betydelse.

3.2 Gemensamt personuppgiftsansvariga

Om flera aktörer tillsammans bestämmer ändamål med och medel för behandlingen av personuppgifter kan de anses vara gemensamt personuppgiftsansvariga, vilket framgår av definitionen i artikel 4.7 dataskyddsförordningen.

Kravet på gemensamt beslutande om ändamål och medel innebär inte att de inblandade aktörerna måste ha lika stor inverkan på besluten om ändamålen för och medel för behandlingen. Det är tillräckligt att en aktör i eget syfte påverkar behandlingen av personuppgifter, och därigenom bidrar till att bestämma ändamål och medel för behandlingen.[9] Det krävs inte heller att var och en av de inblandade aktörerna har åtkomst till de aktuella personuppgifterna.[10] Den som organiserar och samordnar hur andra ska behandla personuppgifter för ett eget syfte kan därför ha ett gemensamt personuppgiftsansvar med dessa.[11] En förutsättning bör dock vara att ändamålen med behandlingen är gemensamma även om de inblandade aktörerna kan ha olika stort intresse av att behandlingen utförs.

När flera aktörer behandlar samma personuppgifter var och en för egna ändamål och utan att det finns ett nära samband mellan dessa ändamål handlar det normalt om självständiga personuppgiftsansvariga. Det utesluter inte att dessa delar personuppgifter med varandra till exempel att en kommun överlämnar en lista på fastighetsägare vars sopor ska hämtas till en firma som sköter sophämtningen. Det gäller åtminstone så länge som överlämnandet endast sker åt ena hållet.

8 HFD 2012 ref. 21.

9 C-25/17, Jehovas vittnen, p. 68.

10 C-25/17, Jehovas vittnen, p. 69, se även HFD 2012 ref. 21.

11 Jfr C-25/17, Jehovas vittnen, p. 71.

EXEMPEL: **ANLITANDE AV REKRYTERINGSFÖRETAG**

Ett företag eller en kommun anlitar ett rekryteringsföretag för att rekrytera ny personal till sin kundtjänst. Företaget överlämnar en kravprofil till rekryteringsföretaget för de tjänster som ska tillsättas men ger inga ytterligare instruktioner för hur de sökandes personuppgifter ska behandlas. Till avtalet med rekryteringsföretaget biläggs ett personuppgiftsbiträdesavtal i vilket det anges att rekryteringsföretaget är personuppgiftsbiträde. Rekryteringsföretaget tar därefter hand om den inledande rekryteringsprocessen med annonsering och ett första urval av de sökande enligt företag/kommunens kravprofil. I arbetet tar rekryteringsföretaget även hjälp av en databas som de själva driver och till vilken arbetssökande kan anmäla sig. Vid kontakter med de arbetssökande som söker tjänsterna på kundtjänsten anger rekryteringsföretaget att de utför arbetet på uppdrag av företag/kommun. Efter utfört arbete överlämnar rekryteringsföretaget en lista till företag/kommun med tänkbara kandidater för intervjuer.

I detta fall är det viktigt att kartlägga och, om möjligt, separera olika behandlingar från varandra. Behandlingen som utförs när rekryteringsföretag samlar in personuppgifter till sin databas för arbetssökande har rekryteringsföretaget ett eget självständigt personuppgiftsansvar för. Ändamålet får i det fallet anses vara att underlätta matchning mellan arbetssökande och arbetsgivare och därigenom bidra till rekryteringsföretagets uppdragsverksamhet. Rekryteringsföretaget bestämmer ensamt över både ändamålen och medlen för behandlingen.

När det gäller behandlingen av personuppgifterna som används i uppdraget kan ändamålet sägas ha formulerats och bestämts av företaget/kommunen. Ändamålet skulle då vara rekrytering av personal till en kundtjänst. Men även rekryteringsbolaget skulle kunna formulera ett eget ändamål, nämligen att ta fram underlag för fullgörandet av uppdraget. Det faktum att företaget/kommunen inte har lämnat några särskilda instruktioner till rekryteringsföretaget för behandlingen av de arbetssökandes personuppgifter innebär att rekryteringsföretaget har fått stort manöverutrymme att själv besluta över behandlingen. Rekryteringsföretaget beslutar själv vilka personuppgifter som ska samlas in och vilka som ska ha åtkomst till uppgifterna. Utförandet av uppdraget innebär också att rekryteringsföretaget använder sin sakkunskap om rekrytering. Detta talar för att rekryteringsbolaget ska anses ha ett eget självständigt personuppgiftsansvar och att det sker ett utlämnande av personuppgifter från en personuppgiftsansvarig till en annan personuppgiftsansvarig när listan på kandidater överlämnas till företaget/kommunen.

Å andra sidan framgår av avtalet att parterna anser att rekryteringsföretaget är ett biträde. Behandlingen skulle heller inte utföras av rekryteringsföretag om inte företaget/kommunen hade begärt uppdraget. Behandlingen av person-

uppgifter är inte centrala i uppdraget men en väsentlig och oundviklig del av uppdraget. De arbetssökande bör dessutom få uppfattningen att rekryteringsföretaget arbetar på företagets/kommunens uppdrag och att det därför är det/den som samlar in deras personuppgifter. Detta talar för att rekryteringsföretaget ska vara ett personuppgiftsbiträde till företaget/kommunen.

Det torde inte vara möjligt att dela upp behandlingen så att kommunen respektive företaget kan bära personuppgiftsansvar för varsin del. För att ge de registrerade, det vill säga de arbetssökande, bästa skydd för sina fri- och rättigheter kan det därför vara lämpligt att betrakta företaget/kommunen och rekryteringsföretaget som gemensamt personuppgiftsansvariga. De är i sådana fall skyldiga att reglera samarbetet genom ett "gemensamt arrangemang" enligt artikel 26 dataskyddsförordningen. Observera även att överföring av personuppgifter från rekryteringsföretagets databas bör betraktas som ett utlämnande mellan två självständiga personuppgiftsansvariga.

Det kan noteras att EU-domstolen under 2018 meddelat två avgöranden som tyder på att domstolen anser att gemensamt personuppgiftsansvar är att föredra i oklara situationer.[12] Skälet kan antas vara att ett gemensamt personuppgiftsansvar ger de registrerade det bästa skyddet för deras fri- och rättigheter.

PRAXIS: WIRTSCHAFTSAKADEMIE

I mål C-210/16, Wirtschaftsakademie Schleswig-Holstein GmbH, konstaterade EU-domstolen att begreppet registeransvarig (personuppgiftsansvarig) enligt dataskyddsdirektivet (som är det direktiv som PUL genomförde) omfattar administratören för en så kallad fanpage som tillhandahålls av ett socialt nätverk (Facebook). Domstolen påpekade att Facebook är den som i första hand bestämmer ändamål och medel för behandlingen av personuppgifterna men ansåg att administratören bidrog till behandlingen, bland annat genom att konfigurera sidan för att ta fram relevant statistik över besökarna av sidan. Att statistiken som Facebook tillhandahöll administratören var anonymiserad saknade betydelse eftersom framtagningen av statistiken förutsätter personuppgiftsbehandling. Bedömningen gjordes utifrån dataskyddsdirektivet men domen har betydelse även för tolkning av dataskyddsförordningen.

12 Se EU-domstolens domar C-210/16 Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388, och C25/17 Jehovas vittnen.

PRAXIS: JEHOVAS VITTNEN

I mål C-25/17, Jehovas vittnen, konstaterade EU-domstolen att samfundet Jehovas vittnen var gemensamt personuppgiftsansvariga med samfundets medlemmar för en behandling av personuppgifter som utfördes när medlemmarna upprättade minnesanteckningar i samband med predikoarbete genom dörrknackning. Minnesanteckningar innehöll uppgifter om vilka personer som inte vill ta emot besök från medlemmarna. Samfundet organiserade och samordnade medlemmarnas predikoarbete och hade kännedom om medlemmarnas insamling av personuppgifter. De insamlade personuppgifterna sammanställdes av samfundet för att upprätta förteckningar. Domstolen ansåg därför att samfundet deltar i att bestämma ändamålet med och medlen för behandlingen. Vidare konstaterade domstolen att det inte krävs att samfundet har tillgång till de aktuella personuppgifterna eller att det har fastställts att samfundet har gett sina medlemmar skriftliga riktlinjer eller instruktioner avseende behandlingen.

3.3 Personuppgiftsbiträde

3.3.1 Behandlar för den personuppgiftsansvariges räkning

Personuppgiftsbiträde (processor) är kortfattat uttryckt den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Enligt definitionen i artikel 4.8 dataskyddsförordningen är personuppgiftsbiträde:

> *”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning”.*

Personuppgiftsbiträdet är i princip alltid en juridisk person. Ett undantag som kan förekomma är enskilda näringsidkare som självständigt behandlar personuppgifter för den personuppgiftsansvariges räkning. Det brukar sägas att personuppgiftsbiträdet alltid ska finnas utanför den personuppgiftsansvariges organisation. Vad som avses är att personuppgiftsbiträdet inte arbetar under den personuppgiftsansvariges överinseende (ledning) såsom anställda och andra så kallade medhjälpare (jämför artikel 29 dataskyddsförordningen). Det utesluter dock inte att personal från personuppgiftsbiträdet kan befinna sig i den personuppgiftsansvariges lokaler och ha tillgång till dennes it-system.

3.3.2 Den som behandlar personuppgifter utan att vara personuppgiftsansvarig

I många fall identifieras ett personuppgiftsbiträde motsatsvis genom ett konstaterande att denne behandlar personuppgifter utan att vara personuppgiftsansvarig. Det betyder att en aktör som behandlar personuppgifter utan att ha något inflytande på ändamålen med behandlingen normalt sett är ett personuppgiftsbiträde. Ett biträde kan, som nämnts ovan, ha fått bestämmanderätt

över medlen för behandlingen vilket omfattar tekniska och organisatoriska frågor såsom vilka IT-system som ska användas och hur de ska konfigureras, men även frågor av större betydelse för personuppgiftsbehandlingen såsom vilka personuppgifter som ska behandlas, vilka som ska ha åtkomst till personuppgifterna, till vilka personuppgifterna ska lämnas ut, och när personuppgifterna ska raderas. Formellt sett sker det genom en delegation från den personuppgiftsansvarige men i praktiken kan det många gånger ske genom att den personuppgiftsansvarige godkänner personuppgiftsbiträdets standardvillkor.

EXEMPEL: **WEBBHOTELL OCH SOCIALA NÄTVERK**

En leverantör av webbhotelltjänster är i princip personuppgiftsbiträde för de personuppgifter som offentliggörs online av de kunder som använder leverantören som värd för sin webbplats och för dess underhåll. Om leverantören vidarebehandlar uppgifterna på webbplatserna för sina egna ändamål blir leverantören personuppgiftsansvarig för just den behandlingen.[13] Det handlar då om två olika behandlingar. Tillhandahållare av sociala nätverk behandlar personuppgifter vanligtvis på det sättet för egna ändamål men kan också bära ett gemensamt personuppgiftsansvar med kunderna.[14]

Ett personuppgiftsbiträde grundar sin rätt att behandla personuppgifter på mandat från den personuppgiftsansvarige. Personuppgiftsbiträdet kan framför allt inte ha någon annan rättslig grund för behandlingen än den som personuppgiftsansvarige stödjer sin behandling på. Det är således en förutsättning att man först identifierar vem eller vilka som är personuppgiftsansvariga.

Det är inte ovanligt att flera personuppgiftsbiträden medverkar i behandlingen, antingen anlitade direkt av en personuppgiftsansvarig eller som underleverantör till ett sådant biträde. I det senare fallet kallas biträdet för underbiträde.

3.3.3 Personuppgiftsbiträdet har litet manöverutrymme

Den som har ett litet manöverutrymme att själv välja när och varför personuppgifter ska behandlas i förhållande till den som beställer en tjänst ska normalt inte anses ha ett eget personuppgiftsansvar. Denne är vanligtvis att betrakta som ett personuppgiftsbiträde i stället. Ett exempel är leverantören av traditionella IT-tjänster såsom tillhandhållandet av en serverhall, lagringskapacitet eller IT-drift. Omfattande instruktioner för personuppgiftsbehandlingen innebär att manöverutrymmet minskar.

Observera att beslut om medlen kan av den personuppgiftsansvarige delegeras till personuppgiftsbiträdet utan närmare instruktioner om hur behandlingens ska

13 Behandlingen kan grunda sig på avtal med kunderna, ske i strid med avtalet eller ske för att uppfylla en författningsreglerad uppgiftsskyldighet.

14 Jfr exempel 16 i Artikel 29-gruppens yttrande 1/2010 om begreppet registeransvarig och registerförare, WP 169.

utföras. I sådana fall är det viktigt att ändamålen har definierats med tillräcklig detaljnivå för att personuppgiftsbiträdet ska kunna bedöma vilken metod som är lämplig för att uppnå ändamålet. Den personuppgiftsansvarige måste också få information om vilka medel som personuppgiftsbiträdet använder.

Begränsat manöverutrymme på grund av instruktioner från en annan aktör ska inte förväxlas med den situation att manöverutrymmet är begränsat på grund av reglering som gäller för aktörens verksamhet, till exempel bankverksamhet. Personuppgiftsbehandlingen inom en bankverksamhet styrs i viss utsträckning av lagreglering vilket minskar bankernas möjlighet att ta emot instruktioner från någon annan. Det talar därför för att banker ofta har ett eget personuppgiftsansvar.

3.3.4 Rättslig skyldighet som åligger personuppgiftsbiträdet

En rättslig skyldighet som åligger ett personuppgiftsbiträde kan innebära att denne måste behandla personuppgifter utan eller i strid med instruktioner från den personuppgiftsansvarige. Så kan vara fallet när en myndighet agerar som personuppgiftsbiträde. Biträdesavtalet och krav på instruktioner från den personuppgiftsansvarige hindrar till exempel inte en myndighet att lämna ut personuppgifter med stöd av 2 kap. tryckfrihetsförordningen (1949:105) om allmänna handlingars offentlighet. Myndigheten blir personuppgiftsansvarig för personuppgiftsbehandlingen som är nödvändig för utlämnandet av allmänna handlingar. Det påverkar dock inte dennes ställning som biträde i förhållandet till den första personuppgiftsansvarige. Ett annat exempel är skyldigheter att anmäla misstänkt penningtvätt enligt penningtvättslagen (lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism). Att biträdet har rätt att utföra sådan behandling utan eller i strid med instruktioner från den personuppgiftsansvarige framgår av artikel 28.3 a dataskyddsförordningen.

EXEMPEL: **REVISIONSBYRÅ**

En revisorsfirma tillhandahåller tjänster till allmänheten och småföretagare på grundval av mycket övergripande instruktioner (”deklarera åt mig”). Revisorsfirman är i detta fall personuppgiftsansvarig. Men om revisorsfirman anlitas av en kommun och får detaljerade instruktioner av kommunens egna revisorer, till exempel för att göra en ingående revision, ska revisorsfirman normalt betraktas som personuppgiftsbiträde, på grund av de tydliga instruktionerna och det begränsade utrymmet för egna beslut. Här finns dock ett viktigt förbehåll, nämligen att när en revisor anser sig ha upptäckt oegentligheter som måste rapporteras, agerar revisorsfirman under eget personuppgiftsansvar, eftersom revisorn uppfyller sina yrkesmässiga skyldigheter.[15]

15 Jfr exempel 23 Artikel 29-gruppens yttrande 1/2010 om begreppet registeransvarig och registerförare, WP 169.

3.3.5 Undvik onödiga personuppgiftsbiträdesavtal

Vid bedömningen av personuppgiftsansvar vid kund-leverantörsförhållanden finns det en tendens att se det faktum att leverantören tillhandahåller en tjänst till kunden som avgörande för att all behandling som därvid aktualiseras utförs för kundens räkning då kunden ytterst kan sägas bestämma ändamål och medel genom att anlita leverantören. Detta synsätt medför förstås att det blir enkelt att fastställa att det är kunden som är personuppgiftsansvarig och leverantören som är personuppgiftsbiträde. Följden av ett sådant synsätt blir dock att ett personuppgiftsbiträdesavtal ska upprättas och ingås mellan parterna och att det ligger på kunden att instruera leverantören om behandlingen av personuppgifter och i övrigt kontrollera och övervaka biträdet för att uppfylla sina skyldigheter som personuppgiftsansvarig. Detta medför en mängd olägenheter för båda parter utan att det nödvändigtvis medför ett bättre skydd för de registrerade.

Som framgår av denna promemoria är det relativt enkelt att konstatera att det i många fall inte handlar om en biträdessituation i kund-leverantörsförhållanden till exempel genom att konstatera att den behandling som leverantören utför vid fullgörande av sina förpliktelser sker för dennes eget intresse (till exempel faktureringsändamål) eller då leverantören har stor frihet att själv bestämma om och hur behandlingen ska utföras. Det är vanligtvis fallet när dennes förpliktelser enligt avtalet huvudsakligen består av något annat än att behandla personuppgifter. Förhållandet mellan kunden och leverantören bör då betraktas som ett utlämnande mellan två personuppgiftsansvariga. Även i dessa fall kan det finnas behov av att klargöra personuppgiftsansvaret men det bör kunna göras förhållandevis enkelt.

3.4 Behandling av anställda och medhjälpares uppgifter

Anställda och andra fysiska personer med liknande ställning som arbetar i den personuppgiftsansvariges eller personuppgiftsbiträdes verksamhet och där behandlar personuppgifter har inget personligt ansvar för personuppgiftsbehandlingen. Detta gäller under förutsättning att de behandlar personuppgifterna under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende. Sådana så kallade medhjälpare får, på samma sätt som personuppgiftsbiträden, behandla personuppgifter endast enligt instruktioner från den personuppgiftsansvarige, artikel 29 dataskyddsförordningen.

Inhyrd person från bemanningsföretag eller så kallade resurskonsulter har vanligtvis ställning som medhjälpare under förutsättning att de agerar under den personuppgiftsansvariges överinseende. Gränsdragningen gentemot mer självständiga konsulter kan vara svår att göra.

PRAXIS: LANDSTINGETS REVISORER

Datainspektionen har i ett samrådsyttrande från 2005 (dnr 2061-2005) ansett att landstingsstyrelsen bär personuppgiftsansvaret för den personuppgiftsbehandling som landstingets egna revisorer utför inom sitt granskningsuppdrag. Datainspektionen påpekade att även om revisorernas granskning ska bedrivas självständigt har revisorerna själva inte befogenhet att behandla personuppgifter för ändamål som ligger utanför granskningsuppdraget. Det var således landstingsstyrelsen som beslöt om ändamål för behandlingen och slöt avtal med eventuella personuppgiftsbiträden som anlitades för revisorernas personuppgiftsbehandling.

3.5 När kommuner anlitar privata utförare och entreprenörer

3.5.1 Kartlägg personuppgiftsbehandlingen

Vid avtal mellan en kommun och privata aktörer uppstår många gånger situationer i vilka det kan vara svårt att bedöma personuppgiftsansvaret. I sådana situationer är det viktigt att inledningsvis kartlägga den aktuella personuppgiftsbehandlingen, se avsnitt 2.

3.5.2 Privata aktörer i samarbete med en kommun

När en kommun överlämnar vården av kommunala angelägenheter till privata utförare medför det vanligtvis att personuppgifter om till exempel kommuninvånare kommer att behandlas av utföraren. En vanlig situation är att utföraren får uppdraget att utföra vård, bedriva skolverksamhet, etcetera utan att kommunen ger några särskilda instruktioner om hur personuppgifterna i verksamheten ska behandlas. Vissa verksamheter såsom skola, vård och socialtjänster, styrs av specialreglering. Ansvaret för att följa sådana verksamhetsspecifika regler ligger i första hand på den privata utföraren. Kommunen har enligt kommunallagen ett ansvar att kontrollera och följa upp verksamheten när kommunala angelägenheter överlämnas till privata utförare. Även när en kommun i andra fall anlitar privata aktörer för att utföra en tjänst kan det vara fråga om att kommunen och den privata aktören bär ett självständigt personuppgiftsansvar.

När en kommun av en privat aktör köper en tjänst som inte huvudsakligen består i att behandla personuppgifter och den privata aktören får ett stort självbestämmande över hur personuppgifterna ska behandlas bär normalt den privata aktören ett eget självständigt personuppgiftsansvar. Även om den privata aktörens valmöjligheter för personuppgiftsbehandlingen begränsas av speciallagstiftning för till exempel skola och vård bär denne normalt personuppgiftsansvaret för den personuppgiftsbehandling som utförs inom verksamheten.

Bedömningen kan dock kompliceras av om aktören i större eller mindre utsträckning integreras i kommunens verksamhet till exempel genom att åläggas att använda ett av kommunen tillhandahållet IT-system för dokumentation eller om det i övrigt förekommer omfattande informationsutbyte mellan kommunen och den privata aktören. Om kommunen dessutom i avtal ställer krav på hur personuppgifterna ska behandlas kan det innebära att den privata aktören är att anse som personuppgiftsbiträde oavsett vad som anges i avtalet.

Om uppdraget innebär att personuppgifter lämnas ut från kommunen till den privata aktören måste således kommunen tillse att utlämnandet följer dataskyddslagstiftningen. Efter överlämnandet av personuppgifter är det den privata aktören som bär personuppgiftsansvaret och som måste tillse att mottagandet och den fortsatta behandlingen uppfyller kraven enligt dataskyddslagstiftningen. Det finns inga uttryckliga krav i dataskyddsförordningen att utlämnande mellan två självständiga personuppgiftsansvariga ska regleras i avtal. Det är dock vår rekommendation att så sker, se mer nedan.

3.5.3 Personuppgiftsansvar inom en kommun

Vid avtal med en kommun är det viktigt att fastställa hur personuppgiftsansvaret fördelas inom kommunen och vilka nämnder som kan sluta avtal i egenskap av personuppgiftsansvarig eller personuppgiftsbiträde.

När behandling av personuppgifter utförs inom en kommun är det vanligtvis kommunstyrelsen eller en kommunal nämnd som bär personuppgiftsansvaret. Förutsättningen för att en nämnd ska bära ett personuppgiftsansvar är att den är tillräckligt självständig i förhållande till kommunstyrelsen. Det medför till exempel att en utbildningsnämnd är personuppgiftsansvarig för personuppgiftsbehandling som sker inom en kommunal skola. Socialnämndens personuppgiftsansvar är särskilt reglerat i förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten.

Om kommunstyrelsen eller en annan nämnd tillhandahåller ett gemensamt IT-system som används av flera nämnder inom en kommun kan den tillhandahållande nämnden anses vara personuppgiftsbiträde åt de nämnderna som använder IT-systemet i sin verksamhet. Normalt bör nämnderna på grund av sekretess vara skyldiga att separera den information som de behandlar inom sin verksamhet. Nämnderna kan i sådana fall vara personuppgiftsansvariga var och en för sin behandling i IT-systemet. Bedömningen kan bli en annan om det är ett IT-system som till exempel används för informationsutbyte mellan nämnderna. I dessa fall kan nämnderna anses vara gemensamt personuppgiftsansvariga.

3.5.4 Reglering av personuppgiftsansvaret inom en kommun

För att bedöma om en kommunal nämnd är personuppgiftsansvarig kan det vara nödvändigt att granska avtal som nämnden ingått med andra nämnder och kommunala reglementen genom vilka kommunfullmäktige beslutar om nämndernas verksamhet.

En kommun har i viss utsträckning möjlighet att fördela och fastställa personuppgiftsansvaret internt inom kommunen. Avtal mellan de inblandade aktörerna och deras uppfattning om personuppgiftsansvaret har, som nämnts ovan, betydelse för vem som ska anses vara personuppgiftsansvarige respektive personuppgiftsbiträde. Även avtal mellan kommunala nämnder eller kommuner bör på samma sätt ha betydelse för personuppgiftsansvaret.

Kommunala reglementen kan ha betydelse för fördelning av personuppgiftsansvaret inom en kommun. Av definitionen av personuppgiftsansvarige i artikel 4.7 dataskyddsförordningen följer att personuppgiftsansvaret kan fastställas i nationell rätt. I en kommun ska kommunfullmäktige anta reglementen om nämndernas verksamhet och arbetsformer (6 kap. 44 § kommunallagen 2017:725). Kommunala reglementen bör därför kunna användas för att fastställa personuppgiftansvaret inom en kommun.

Kommunala reglementen kan även ersätta ett personuppgiftsbiträdesavtal när en kommunal nämnd ska agera som personuppgiftsbiträde åt andra kommunala nämnder. Reglementet är en sådan ”annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet” som enligt artikel 28.3 dataskyddsförordningen kan ersätta avtalsregleringen mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

Om flera kommunala nämnder inom samma kommun anses vara gemensamt personuppgiftsansvarige bör deras inbördes relation kunna fastställas i ett kommunalt reglemente, jämför artikel 26 dataskyddsförordningen.

Vid kommunalt samarbete, det vill säga mellan två eller flera kommuner, kan avtal och reglementen vara av betydelse för att fastställa personuppgiftsansvaret.

3.5.5 Villkoren för personuppgiftsbehandlingen måste klargöras i upphandlingsunderlaget

Det är, som nämnts ovan, väsentligt att fördelningen av personuppgiftsansvaret klargörs och dokumenteras innan kommunen överlämnar en kommunal angelägenhet till en privat aktör eller annars låter en privat aktör att utföra arbete åt kommunen som innebär att personuppgifter kommer att hanteras.

Redan i upphandlingsunderlaget bör därför kommunen beskriva den personuppgiftsbehandling som krävs vid utförandet av den upphandlade verksamheten och hur ansvaret ska fördelas. Kommunen kan i en sådan beskrivning inte fördela personuppgiftsansvaret på ett sätt som strider mot dataskyddslagstiftningen. I komplicerade situationer där det är oklart hur ansvaret ska fördelas kan parternas uppfattning av placering av personuppgiftsansvaret tillmätas betydelse.

Upphandlingsunderlaget bör ange hur personuppgiftsansvaret ska fördelas mellan de inblandade parterna, det vill säga om den privata aktören enligt kommunens uppfattning är ett personuppgiftsbiträde eller om denne ska anses bära ett eget personuppgiftsansvar. För det fallet att den privata aktören är personuppgiftsbiträde bör utkastet till personuppgiftsbiträdesavtalet finnas med

i upphandlingsunderlaget så att den privata aktören kan göra en juridisk och kommersiell bedömning av personuppgiftsbiträdesavtalet. Även instruktioner och krav på till exempel tekniska och organisatoriska åtgärder för säkerhet såsom skyddad kommunikation via öppna nät, åtkomstkontroll och gallring bör anges.

Instruktioner om personuppgiftsbehandlingen i upphandlingsunderlaget kan påverka bedömningen av fördelning av personuppgiftsansvaret. Omfattande instruktioner som innebär minskat manöverutrymme för den privata aktören talar för att denne är att betrakta som ett personuppgiftsbiträde. Men instruktioner i upphandlingsunderlaget kan även förekomma när det handlar om en överföring av personuppgifter till en aktör som bär ett eget personuppgiftsansvar. Kommunen måste nämligen försäkra sig om att överföringen av personuppgifter till en annan personuppgiftsansvarig är laglig och kan av det skälet behöva ställa krav på överföringen och vad uppgifterna ska användas till.

Om den privata aktören i en upphandlingssituation anser att kommunen har gjort en felaktig bedömning av fördelningen av personuppgiftsansvaret kan den privata aktören delge sin ståndpunkt till kommunen, exempelvis inom ramen för ”frågor och svar” i upphandlingen. Den privata aktören kan då redogöra för sin egen uppfattning och antingen be kommunen att ändra sin uppfattning eller motivera sitt ställningstagande. Om kommunen ändrar sin uppfattning, och det innebär att ändringen av fördelningen av personuppgiftsansvar utgör en väsentlig ändring i upphandlingslagstiftningens mening, måste kommunen förlänga anbudstiden i upphandlingen (11 kap. 8 § lag (2016:1145) om offentlig upphandling, LOU. Om ändringen är så pass ingripande att upphandlingens art ändras måste kommunen enligt förarbetena till LOU istället annonsera upphandlingen på nytt (prop. 2015/16:195, s. 1064).

4. Reglera och dokumentera förhållandet mellan aktörerna

4.1 Oftast ett krav att reglera ansvaret

När ansvarsfördelningen är bedömd och fastställd är nästa steg att överväga att reglera förhållandet mellan de inblandade aktörerna i ett avtal. Bortsett från situationen när det handlar om en överföring från en självständigt personuppgiftsansvarig till en annan självständigt personuppgiftsansvarig är det dessutom ett krav enligt dataskyddsförordningen att reglera förhållandet. Även vid sådan överföring är det dock en stark rekommendation att reglera förutsättningarna för överföringen. Omfattningen av regleringen kan dock variera beroende på hur komplex behandlingssituationen är och riskerna med behandlingen.

4.2 Avtal för utlämnande till självständig personuppgiftsansvarig

Något krav enligt dataskyddsförordningen på att avtalsreglera denna typ av situation finns inte. Däremot är det ofta en god idé att göra det, särskilt i komplicerade behandlingssituationer eller om behandlingen medför särskilda risker för de registrerade eller de inblandade aktörerna.

Den part som lämnar ut uppgifterna bör säkerställa att den mottagande parten åtar sig att behandla personuppgifterna enligt dataskyddsreglerna. För att kunna göra en bedömning om utlämnande av personuppgifterna är förenligt med de ändamål för vilka personuppgifterna samlades in, kan det även finnas behov av att få information om för vilka ändamål den mottagande parten avser att behandla personuppgifterna och om dennes verksamhet i övrigt.

Den mottagande parten bör i sin tur i vart fall försäkra sig om att de registrerade är korrekt informerade om personuppgiftsbehandlingen som utlämnandet innebär och att insamlingen av deras personuppgifter i övrigt har varit laglig. För bedömning av den egna behandlingen kan den mottaganden parten även ha behov av att känna till för vilka ändamål som personuppgifterna samlades in och med vilken rättslig grund som insamlingen genomfördes.

Beroende på de faktiska omständigheterna i den enskilda situationen kan det innebära att både parterna och de registrerade upplever det som enklare och bättre om även ytterligare åtgärder såsom informationslämning och hantering av de enskildas rättigheter med mera hanteras gemensamt av de personuppgiftsansvariga. En avtalsreglering av detta menar vi kan hanteras genom ingående av ett datadelningsavtal, vilket beskrivs närmare nedan.

4.3 Inbördes arrangemang för gemensamt personuppgiftsansvar

Om personuppgiftsansvaret är gemensamt för en eller flera behandlingar ålägger dataskyddsförordningen de personuppgiftsansvariga att ingå ett ”inbördes arrangemang”, artikel 26 dataskyddsförordningen. Av det inbördes arrangemanget ska särskilt former och ansvar för utövande av den registrerades rättigheter och skyldigheten att lämna information till registrerade framgå. Arrangemanget ska också ”på lämpligt sätt återspegla gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade” samt att ”det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade”. Vår uppfattning är att kraven på ett inbördes arrangemang lämpligen kan uppfyllas genom ingående av ett så kallat datadelningsavtal. Ett sådant datadelningsavtal bör innehålla åtminstone följande avsnitt:

- ❑ Klargörande av de olika aktörerna och deras roller.
- ❑ Varför data behandlas (ändamålet).
- ❑ Vilken typ av data som ska/får omfattas.
- ❑ Hur de registrerade kan utöva sina rättigheter.
- ❑ Hur de registrerade ska få tillräcklig information om behandlingen.
- ❑ Hur de grundläggande principerna för behandling av personuppgifter uppfylls.
- ❑ Laglig grund för behandlingen.
- ❑ Om någon av de ansvariga ska utgöra en gemensam kontaktpunkt för de registrerade med mera.

Andra viktiga frågor som kan vara lämpliga att adressera är gallring, säkerhet i behandlingen, sekretess och möjligheterna till kontroll av den andre partens avtalsefterlevnad. Det är även lämpligt att adressera fördelningen av ansvar för skadestånd och andra krav, inklusive administrativa sanktionsavgifter.

I komplicerade situationer, där det exempelvis finns ett större antal aktörer (som ömsom kan vara ensamt personuppgiftsansvariga, gemensamt personuppgiftsansvariga och även biträden) går datadelningsavtal att konstruera på ett sätt som även inkluderar personuppgiftsbiträdesavtal samt möjligheten att genom fullmakt ingå personuppgiftsbiträdesavtal med externa biträden för datadelningsavtalets deltagande aktörers räkning.

4.4 Biträdesavtal och avtal med underbiträden

Om en behandling innebär en biträdesrelation måste, enligt artikel 28 dataskyddsförordningen, den personuppgiftsansvarige och personuppgiftsbiträdet ingå ett biträdesavtal. Även under PUL var det obligatoriskt att ingå

biträdesavtal, men i och med införandet av personuppgiftbiträdenas självständiga ansvar enligt artikel 82.2 dataskyddsförordningen, har biträdesavtal blivit föremål för betydligt mer omfattande förhandling. De legala kraven på vad ett biträdesavtal ska innehålla är för svensk del i stort sett en kodifiering av praxis och framgår uttryckligen av främst artikel 28 dataskyddsförordningen. Det juridiska innehållet i ett personuppgiftbiträdesavtal är därför i bästa fall inte föremål för alltför omfattande förhandlingar.

4.5 Instruktioner till medhjälpare

Även vad gäller medhjälpare, vilket oftast innebär anställda eller andra som arbetar under en personuppgiftsansvarigs eller ett personuppgiftbiträdes överinseende, uppställer dataskyddsförordningen krav på hur detta ska hanteras. Enligt artikel 29 dataskyddsförordningen får medhjälpare nämligen endast behandla personuppgifter på instruktion från den personuppgiftsansvarige, om inte annat följer av lag. Instruktionerna behöver inte vara skriftliga men av uppenbara skäl, främst ut bevissäkringssynpunkt, bör de ofta vara det. Enligt artikel 32.4 dataskyddsförordningen är det den personuppgiftsansvarige som är ansvarig för att tillräckliga instruktioner finns.

5. Checklistor för personuppgiftsansvar

5.1 Kartlägg behandlingen eller behandlingarna

I mer komplicerade situationer där behandling utförs av flera aktörer för helt eller delvis gemensamma intressen kan det vara lämpligt att som ett inledande steg kartlägga behandlingen eller behandlingarna.

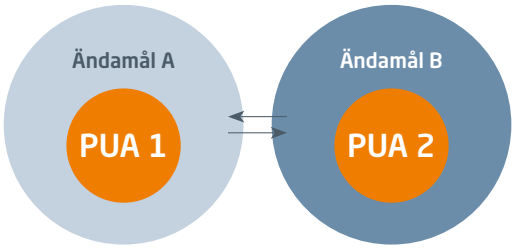
- ❑ Vilket eller vilka är ändamålen med behandlingen, det vill säga varför behandlas personuppgifterna?
- ❑ Vilka kategorier av personuppgifter behandlas?
- ❑ Vilka kategorier av registrerade omfattas av behandlingen?
- ❑ Beskriv hur personuppgifterna hanteras (flödet), varifrån de samlas in, vilka som har tillgång till dem, hur de lämnas ut och när de ska raderas.
- ❑ Identifiera samtliga aktörer som är inblandade i behandlingen.

5.2 Fastställ personuppgiftsansvaret

När flera aktörer är inblandade i behandling av personuppgifter och utbyter personuppgifter med varandra kan personuppgiftsansvaret fördelas på följande sätt. Bestämmanderätten över ändamålen är avgörande för fördelningen.

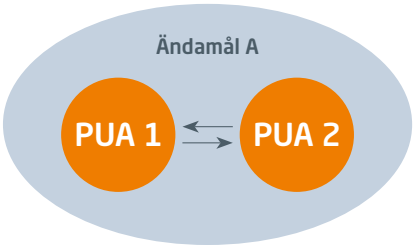
Situation A

Självständiga personuppgiftsansvariga med olika ändamål och samordnad behandling som innebär ett utlämnande.



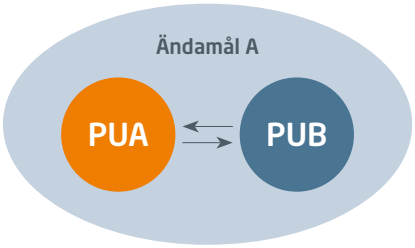
Situation B

Gemensamt personuppgiftsansvariga (PUA).



Situation C

En ensamt personuppgiftsansvarig (PUA) med personuppgiftsbiträde (PUB)



5.2.1 Faktorer som talar för ett eget självständigt personuppgiftsansvar

- ❑ Aktören bestämmer varför och hur personuppgifterna ska behandlas.
- ❑ Personuppgifterna behandlas endast för aktörens egna intressen (ändamål).
- ❑ Aktören har ett eget intresse av att behandlingen utförs.
- ❑ Aktören tar initiativ till att behandlingen utförs.
- ❑ Behandlingen kommer inte att utföras utan aktörens initiativ och utfärdande av instruktioner för behandlingen.
- ❑ Den andra aktören behandlar personuppgifter endast för den första aktörens räkning och har inget eget intresse av att behandlingen utförs (förutom att leverera tjänsten).
- ❑ Aktören är ålagd enligt lag eller annan författning en arbetsuppgift som medför att det är nödvändigt att behandla personuppgifter.
- ❑ Aktören beslutar om varför (ändamål) och hur (medlen) behandlingen ska utföras och kan delegera beslut om tekniska och organisatoriska frågor.
- ❑ Aktören bestämmer när uppgifter ska rättas eller raderas efter begäran från den registrerade.
- ❑ Aktören kontrollerar att dennes instruktioner för behandlingen efterlevs av andra aktörer.
- ❑ Vid utförande av ett avtal är aktörens huvudsakliga förpliktelse något annat än behandling av personuppgifter och förutsätter dennes sakkunskap inom dennes expertområde.
- ❑ Aktören har gett en annan aktör instruktioner för hur behandlingen av personuppgifter ska utföras (det vill säga inte instruktioner om uppdraget i övrigt ska utföras).
- ❑ Den uppgift som aktören har gett en annan aktör i uppdrag att utföra skulle i princip kunna utföras av aktören själv.
- ❑ De registrerade får en bild av att det är aktören som är personuppgifts-ansvarig.
- ❑ Aktören kan kräva att personuppgifterna återlämnas eller raderas hos den andra aktören när förhållandet avslutas.

5.2.2 Faktorer som talar för ett gemensamt personuppgiftsansvar

- ❑ Flera aktörer har påverkan på beslut om ändamål och medel, det vill säga varför och hur personuppgifterna ska behandlas.
- ❑ Samtliga inblandade aktörer har ett gemensamt intresse av att behandlingen utförs eller egna närliggande intressen av att behandlingen utförs.
- ❑ De olika behandlingsåtgärder som de inblandade aktörerna utför för samma eller närliggande ändamål är så nära sammanbundna att de inte går att separera från varandra.
- ❑ De registrerade får det bästa skyddet för sina fri- och rättigheter genom att kunna vända sig till samtliga gemensamt personuppgiftsansvariga.

5.2.3 Faktorer talar för ett ansvar som personuppgiftsbiträde

- ❑ Aktören behandlar personuppgifter endast för den personuppgiftsansvariges räkning och har i princip inget eget intresse av att behandlingen utförs (utöver att leverera tjänsten till den andra aktören).
- ❑ Aktören har inget inflytande över besluten varför eller hur personuppgifterna behandlas.
- ❑ Aktören har på grund av detaljerade instruktioner från annan aktör ett begränsat manöverutrymme att bestämma över verksamheten i vilken behandlingen av personuppgifterna förekommer och behandlingen i sig.
- ❑ Aktören kan påverka besluten om hur personuppgifterna behandlas, men det sker genom delegation från en annan aktör eller genom att en annan aktör har accepterat den första aktörens standardavtal.
- ❑ Aktören skulle inte behandla de aktuella personuppgifterna om inte denne hade fått begäran från någon annan att göra det.
- ❑ Aktören utför en behandling som är nödvändig för en arbetsuppgift som någon annan är ålagd enligt lag eller annan författning.
- ❑ Aktören har ingen påverkan på beslut om när personuppgifter ska rättas eller raderas efter begäran från den registrerade.
- ❑ Aktören har fått instruktioner om hur behandlingen av personuppgifter ska utföras och en annan aktör kontrollerar att instruktionerna följs.
- ❑ Den behandling av personuppgifter som aktören utför skulle kunna utföras av någon annan.
- ❑ De registrerade får inte en bild av att aktören är personuppgiftsansvarig.
- ❑ Aktören är skyldig att radera eller återlämna personuppgifterna när ett avtal med en annan aktör avslutas.

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00

Grafisk form: **Alida Form**