Behövs biträdesavtal internt inom den kommunala förvaltningen?

Det kommer återkommande frågor kring biträdesavtal och om det behövs internt inom den kommunala förvaltningen eller om det finns andra lösningar. I texten nedan fördjupar vi oss i ämnet och ger våra rekommendationer.

Beträffande frågan om avtal eller rättsakt med personuppgiftsbiträden fastställer artikel 28 dataskyddsförordningen, att båda lösningarna kan användas. Den personuppgiftsansvarige nämnden ska binda sitt personuppgiftsbiträde dvs. den andra nämnden till de krav som räknas upp i artikeln men eftersom kommunen är en juridisk person så kan den inte rent civilrättsligt ingå avtal med sig själv enligt SKLs uppfattning.

Artikel 28.3 i dataskyddsförordningen anger att ”*[n]är uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige…*”

I tidigare praxis har det uttalats att man bör ha avtal mellan olika nämnder i samma kommun. SKL anser att en ”rättsakt” kan användas istället för ett civilrättsligt avtal. Varje personuppgiftsansvarig nämnd måste dock bland annat följa de grundläggande principerna för behandling av personuppgifter (artikel 5) och ha en rättslig grund för behandlingen (artikel 6).

Det är även varje personuppgiftsansvarigs nämndens skyldighet att ge instruktioner till personuppgiftsbiträdes nämnden avseende den behandling som de som personuppgiftsbiträde ska utföra för den personuppgiftsansvarige nämndens räkning.

Detta innebär att man i ett reglemente kan ange vilka nämnder som ska vara personuppgiftsansvariga för olika behandlingar i kommunens system. Den ordningen innebär således att man inte behöver ha biträdesavtal mellan nämnder.

När det gäller kommunövergripande system rekommenderas att man i förteckningen över behandlingsändamål enligt artikel 30 låter KS vara personuppgiftsansvarig för t.ex. all HR-behandling, all epost och övriga kommunövergripande system som används av alla nämnder. På motsvarande sätt bör andra nämnders ansvar även anges i registerförteckningarna.

Det bör notera att personuppgiftsbiträdet bara får behandla personuppgifterna enligt de dokumenterade instruktionerna från den personuppgiftsansvarige nämnden. Det måste finnas instruktioner och personuppgifts-biträdes nämnden behandling får enbart utföras enligt den personuppgiftsansvariges nämndens instruktion.

Ett förtydligande kring personuppgiftsbiträdesavtal

Sveriges Kommuner och Landsting

Vi återkommer med anledning en av önskan om en fördjupning av svaret på frågan om *personuppgiftsbiträdesavtal enligt artikel 28 GDPR behövs inom en kommunala förvaltning.*

Det har tidigare uttalats att både kommunstyrelsen och de kommunala nämnderna – förutsatt att de är så självständiga att de är förvaltningsmyndigheter – var för sig bör anses som personuppgiftsansvarig i sin verksamhet. Vilket organ i kommunen som är personuppgiftsansvarig kan variera; de faktiska omständigheterna måste prövas i varje enskilt fall, till exempel om nämnden självständigt förfogar över de personuppgifter som behandlas.

En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar är inte personuppgiftsbiträde. Ett personuppgiftsbiträde kan vara en fysisk eller en juridisk person och finns alltid utanför den egna organisationen. Om en personuppgiftsbiträdesrelation kan identifieras ska personuppgiftsansvarig enligt artikel 28 punkt 3 reglera hanteringen genom *ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet.* I denna dokumentation ska framgå föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges.

Den omständigheten att GDPR nu innehåller (artikel 26) särskilda bestämmelser för reglering av ett gemensamt personuppgiftsansvar får ses som en anpassning till verkligheten. Det är sannolikt så att många behandlingar som ansetts ha en personuppgiftsansvarig tidigare kan komma att behöva omprövas och anpassas till den mer nyanserade och enskilda bedömning som måste göras i enlighet med GDPR. Det gemensamma personuppgiftsansvaret kommer att få större betydelse och styra personuppgiftsansvarigas agerande i större utsträckning under GDPR. Detta gäller särskilt för de ”koncerngemensamma” systemen diariet, lönesystemet, ekonomisystemet, skrivarna, telefonisystemet m.m.

Av definitionen av personuppgiftsansvarig i GDPR följer att personuppgiftsansvaret kan bäras av en aktör ensamt eller av flera aktörer gemensamt. Om flera aktörer är inblandade i *samma eller närliggande behandlingar* av personuppgifter måste det utredas vilken eller vilka av dessa aktörer som är personuppgiftsansvarig för behandlingen, så att aktören eller aktörerna kan tillse att skyldigheterna under GDPR som åligger personuppgifts-ansvarig uppfylls. Den personuppgiftsansvarige har per definition bestämmanderätt över ändamålen och medlen för behandlingen. Motsatsvis innebär det att en aktör som de facto bestämmer över ändamål och medel inte kan vara personuppgiftsbiträde för den behandlingen.

Med rätten att bestämma över ändamål och medel avses rätten att bestämma över *varför* och *hur* en behandling ska utföras. Viktiga omständigheter för att avgöra graden av bestämmande är vem som är initiativtagare till behandlingen. När det gäller rätten att bestämma över ändamål så är den aktör som har sådan bestämmanderätt alltid personuppgiftsansvarig för den behandlingen, antingen ensamt eller gemensamt med annan.

Graden av självbestämmande och manöverutrymme i beslutsfattandet utgör viktiga parametrar för att avgöra bestämmanderätten. Denna kan grunda sig på faktiskt inflytande över behandlingen. Utifrån avtal eller *annan dokumentation* t.ex. instruktioner kring aktörernas förhållanden är det ofta möjligt att utläsa om en aktör har bestämmanderätt eller en dominerande roll med avseende på behandlingen. Förutsatt att en sådan ordning återspeglar de faktiska omständigheterna vid behandlingen finns det skäl att godta den som avgörande för graden av bestämmande.

Av artikel 26 GDPR framgår att gemensamt personuppgiftsansvariga ”under öppna former ska fastställa sitt respektive ansvar för att fullgöra skyldigheterna” enligt GDPR genom ett inbördes ”arrangemang”. Arrangemanget ska särskilt avse former och ansvar för utövande av den registrerades rättigheter och skyldigheten att lämna information till registrerade. Vidare gäller att arrangemanget ”på lämpligt sätt ska återspegla gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade” samt att ”det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade”.

Kravet på ett arrangemang innebär inte ett uttryckligt krav på avtal aktörerna sinsemellan. Ett sådant arrangemang bör dock dokumenteras skriftligt. Innehållet i det inbördes arrangemanget måste anpassas till de rådande omständigheterna. I vissa fall kan det vara tillräckligt att reglera samverkan/datautbytet i ett tjänsteavtal/överenskommelse mellan parterna vars uppfyllande medför personuppgiftsbehandling. I andra fall kan det vara lämpligt med ett fristående och mera omfattande datadelningsavtal/överenskommelse. Ett datadelningsavtal/överenskommelse som syftar till att personuppgiftsansvaret ska vara intakt, bör föreskriva enhällighet kring beslut som berör den gemensamma personuppgiftsbehandlingen.