

Kommentarer till särskilda bestämmelser för behandlingen av personuppgifter

Utgivet av IT&Telekomföretagen 2017

Dessa kommentarer är avsedda att underlätta användningen av särskilda bestämmelser för behandlingen av personuppgifter. De förklarar också vissa frågor i anslutning till de särskilda bestämmelserna men är inte en del av själva avtalet.

De särskilda bestämmelserna för behandlingen av personuppgifter är avsedda att användas tillsammans med IT&Telekomföretagens allmänna bestämmelser för aktuellt uppdrag, underhåll eller tjänst. De särskilda bestämmelserna för behandlingen av personuppgifter ersätter de allmänna bestämmelsernas villkor om behandlingen av personuppgifter när dataskyddsförordningen börjar tillämpas den 25 maj 2018. Redan ingångna avtal bör därför omförhandlas för att ta höjd för de nya kraven i dataskyddsförordningen, exempelvis genom att parterna bilägger de särskilda bestämmelserna för behandlingen av personuppgifter till parternas befintliga avtal.

Det finns tre versioner av särskilda bestämmelser för behandlingen av personuppgifter; en för Molntjänster, en för IT-Infrastruktur tjänster och en för övriga tjänster (t.ex. IT-Projekt, IT-Tjänster och Agila Projekt). Välj därför de särskilda bestämmelser för behandlingen av personuppgifter som lämpar sig bäst för aktuell(t) tjänst/uppdrag/underhåll.

Till de särskilda bestämmelserna för behandlingen av personuppgifter hör bilagan "Specifikation över behandlingen av personuppgifter". Den bilagan är det viktigt att parterna fyller i senast i samband med att avtalet ingås. Denna kommenteras mer utförligt nedan.

Varför särskilda bestämmelser?

Den 25 maj 2018 börjar dataskyddsförordningen tillämpas i Sverige och övriga EU- och EES-länder. Dataskyddsförordningen ersätter samma dag den svenska personuppgiftslagen som då upphör att gälla.

Dataskyddsförordningen ställer mer omfattande krav på behandlingen av personuppgifter. Exempelvis får en leverantör, i egenskap av personuppgiftsbiträde, ett självständigt ansvar för att säkerställa att de personuppgifter som behandlas skyddas mot oavsiktlig eller olovlig åtkomst, ändring, förstöring, förlust eller röjande. Leverantörer ansvarar också för att säkerställa att det finns en laglig grund för s.k. tredjelandsoverföringar, dvs överföringar av personuppgifter till ett land utanför EU/EES.

Vid sidan av det utökade ansvaret ställer dataskyddsförordningen mer omfattande krav på utformningen av personuppgiftsbiträdesavtal.

IT&Telekomföretagens särskilda bestämmelser för behandlingen av personuppgifter med bilaga, det s.k. Biträdesavtalet, har tagits fram för att möta dessa nya krav.

Om du vill ta del av dataskyddsförordningen kan du göra det här (länk till officiell lagtext):

<http://eur-lex.europa.eu/legal-con-tent/SV/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

Användningsområde

Biträdesavtalet är tänkt att användas när leverantören ska lagra eller på annat sätt behandla personuppgifter för kundens räkning. Om leverantören endast ska behandla data som inte utgör personuppgifter, t.ex. finansiell data, behöver parterna inte bilägga Biträdesavtalet till avtalet.

Biträdesavtalet finns i tre versioner; en för Molntjänster, en för IT-Infrastruktur tjänster

och en för övriga tjänster (t.ex. IT-Projekt, IT-Tjänster och Agila Projekt).

Biträdesavtalet för Molntjänster och IT-Infrastrukturtjänster är till stor del lika, men innehåller vissa avvikelser som beror på tjänsternas karaktärer. Exempelvis har en molntjänstleverantör enligt punkt 3.1.4 en mer långtgående rätt att neka nya instruktioner från kunden än en leverantör av IT-infrastrukturtjänster. Av punkt 3.4.2 framgår bl.a. att kundens kostnad för att frånträda avtalet i vissa fall beräknas på olika sätt. Även ansvarsbegränsningen i punkt 7 skiljer sig åt.

Biträdesavtalet för övriga tjänster (t.ex. IT-Projekt, IT-Tjänster och Agila Projekt) motsvarar i allt väsentligt Biträdesavtalen för Molntjänster och IT-Infrastrukturtjänster, men innehåller vissa skillnader som beror på att den personuppgiftsbehandling som sker i samband med övriga tjänster ofta är begränsad i tid och omfattning. Det förekommer även i högre utsträckning att den aktuella tjänsten utförs i kundens egna lokaler, vilket avspeglas i Biträdesavtalet för övriga tjänster.

Tillämplighet

Både nuvarande personuppgiftslag och kommande dataskyddsförordning kräver att kunden (i egenskap av personuppgiftsansvarig) och leverantören (i egenskap av personuppgiftsbiträde) ingår ett skriftligt personuppgiftsbiträdesavtal.

Idag framgår detta av de allmänna bestämmelserna, men när dataskyddsförordningen börjar tillämpas kommer de allmänna bestämmelsernas villkor om behandlingen av personuppgifter att behöva ersättas av Biträdesavtalet. Detta för att leverantörens behandling av kundens personuppgifter även fortsättningsvis ska vara laglig.

Om parterna bilägger Biträdesavtalet till avtalet kommer Biträdesavtalet att börja gälla från och med den 25 maj 2018 om parterna inte kommer överens om annat. Biträdesavtalet ersätter då de allmänna bestämmelsernas villkor om behandlingen av personuppgifter som gäller mellan parterna fram till den 25 maj 2018.

Uppbyggnad och översiktlig beskrivning

Biträdesavtalet utgör bilaga till avtalet och ska användas tillsammans med tillämpliga allmänna bestämmelser om parterna inte kommer överens om annat.

Enligt Biträdesavtalet är kunden "personuppgiftsansvarig" och leverantören "personuppgiftsbiträde" för behandlingen av personuppgifter under avtalet.

Eftersom leverantören som personuppgiftsbiträde enligt lag inte får behandla personuppgifter för egen räkning kräver Biträdesavtalet att kundens samtliga skriftliga instruktioner preciseras i bilagan "Specifikation över behandlingen av personuppgifter". Bilagan ska parterna fylla i senast i samband med att avtalet ingås. Vilken information som ska fyllas i framgår nedan under avsnittet Bilagan "Specifikation över behandlingen av personuppgifter". Det är viktigt att bilagan är korrekt och tydligt ifylld så att det inte uppstår några oklarheter. Biträdesavtalet för övriga tjänster har i punkt 3.1.1 en s.k. "fall back" reglering utifall parterna av något skäl missar att fylla i bilagan. Biträdesavtalet för Molntjänster och IT-Infrastrukturtjänster innehåller inte en sådan reglering eftersom tjänsterna till sin natur kräver en specificerad instruktion.

Biträdesavtalen beaktar inte bransch- eller sektorspecifik lagstiftning, t.ex. för banker eller organisationer inom hälso- och sjukvården (se mer om definitionen Tillämplig Dataskyddslagstiftning under rubriken "Definitioner av olika begrepp").

Om kunden vill ändra överenskomna instruktioner eller säkerhetsåtgärder har leverantören enligt punkt 3.1.4 respektive 3.2.3 rätt till skälig ersättning, även om ändringen beror på förändringar i Tillämplig Dataskyddslagstiftning. Ändringen ska dokumenteras; företrädesvis genom att parterna uppdaterar bilagan "Specifikation över behandlingen av personuppgifter". Punkten 3.2.4 reglerar särskilt vad som gäller om leverantören under avtalstiden upptäcker att avtalade säkerhetsåtgärder inte uppfyller Tillämplig Dataskyddslagstiftning.

Enligt dataskyddsförordningen är leverantören, i egenskap av personuppgiftsbiträde, skyldig att ersätta registrerade, dvs de personer vars personuppgifter behandlas under avtalet, för skada som uppkommit till följd av behandlingen. Skyldigheten gäller dock bara om leverantören i) inte har fullgjort sina lagliga skyldigheter eller ii) har agerat utanför eller i strid med kundens, dvs den personuppgiftsansvariges lagenliga anvisningar. Enligt dataskyddsförordningen är kunden alltid skyldig att ersätta registrerade för skada som denne orsakat genom behandlingen.

Det bör betonas att Biträdesavtalet inte hindrar att en registrerad kräver leverantören på skadestånd för skada som både kunden och leverantören orsakat. Enligt dataskyddsförordningen kan en registrerad välja vilken part den vill kräva på skadestånd om båda parter har medverkat till skadan. Den part som krävs på skadestånd kan därför bli tvungen att betala ett högre skadestånd än vad som motsvarar dess ansvar enligt dataskyddsförordningen ("överskjutande skadestånd"). Den parten har dock en laglig rätt att regressvis återkräva sådant "överskjutande skadestånd".

Biträdesavtalet reglerar i punkt 7.1 respektive punkt 7.2 uteslutande parts rätt att återkräva en del av det utdömda och utbetalade "överskjutande skadeståndet", inklusive rättegångskostnader, från den andre parten i de fall båda parter medverkat till skadan. Kundens rätt att regressa är i Biträdesavtalet begränsad till ett visst belopp. Vid leverantörens regress mot kunden är kundens ansvar obegränsat.

Leverantörens regress enligt punkt 7.1 innebär en rätt att kräva ersättning av kunden för belopp som överstiger vad leverantören lagligen är skyldig att utge till de registrerade. Det finns med andra ord ingen begränsning för vad leverantören kan vara skyldig att utge direkt till de registrerade. Önskar leverantören ersättas av kunden för sådan utgiven ersättning behöver leverantören lägga till en skadeslöshetsbestämmelse i avtalet.

Punkt 7.4 anger vad parterna måste beakta vid skadeståndskrav från registrerade och punkt

7.5 klargör att parts ansvar för andra typer av skador än de som uttryckligen regleras i punkt 7, t.ex. administrativa sanktionsavgifter, regleras av de allmänna bestämmelserna.

Biträdesavtalet gäller så länge leverantören behandlar personuppgifter för kundens räkning, dvs även efter att avtalet har sagts upp eller i övrigt upphört att gälla. Biträdesavtalet upphör att gälla först när leverantören enligt kundens instruktion har återlämnat eller raderat personuppgifterna från sin IT-miljö och sina backuper. Om leverantören ska fortsätta att lagra backuper efter avtalstidens utgång får parterna komma överens om det separat.

Definitioner av olika begrepp

Under punkt 1 i Biträdesavtalet definieras ett antal nyckelbegrepp som återkommer i Biträdesavtalet. Begreppet Biträdesavtalet har kortfattat kommenterats ovan. Biträdesavtalet hänvisar på flera ställen till "Tillämplig Data-skyddslagstiftning". Med "Tillämplig Data-skyddslagstiftning" förstås, om annat inte överenskommits särskilt, dataskyddsförordningen, dataskyddslagen i Sverige och Datainspektionens bindande föreskrifter och beslut som är tillämpliga på den behandling av personuppgifter som kommer att ske under avtalet.

Innebörden av övriga begrepp, som inte definierats i de allmänna bestämmelserna, ska tolkas i enlighet med Tillämplig Data-skyddslagstiftning. Exempel på sådana begrepp eller koncept är personuppgifter, radering av personuppgifter och personuppgiftsincidenter.

Biträdesavtalet och de allmänna bestämmelserna

Biträdesavtalet och de allmänna bestämmelserna gäller om annat inte överenskommits. Parterna kan givetvis överenskomma om ändringar eller kompletteringar till Biträdesavtalet och de allmänna bestämmelserna. Allt som parterna kommer överens om som framgår av själva avtalsdokumentet eller av andra bilagor har företräde framför Biträdesavtalet och de allmänna bestämmelserna.

Om parterna önskar ersätta de allmänna bestämmelserna med andra avtalsvillkor görs

det enklast genom att parterna i avtalet ändrar definitionen av "Allmänna Bestämmelser". Biträdesavtalet har dock utformats för att tillämpas tillsammans med IT&Telekomföretagens allmänna bestämmelser.

Bilagan "Specifikation över behandlingen av personuppgifter"

Biträdesavtalet är inte komplett utan bilagan "Specifikation över behandlingen av personuppgifter". Det har tidigare poängterats vikten av att bilagan fylls i på ett korrekt och tydligt sätt.

I bilagan ska parterna ange kundens skriftliga instruktioner för den aktuella behandlingen. Bilagan måste därför innehålla information om bl.a. föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och vilka kategorier av registrerade som leverantören ska behandla personuppgifter om.

Eftersom dataskyddsförordningen ger båda parter, inte bara kunden, ett ansvar för att säkerställa att personuppgifterna omfattas av lämpliga säkerhetsåtgärder, bör parterna i bilagan tydliggöra vilka organisatoriska och tekniska säkerhetsåtgärder som är nödvändiga för att skydda de personuppgifter som ska behandlas.

Bilagan bör även innehålla information om vilka underleverantörer, s.k. underbiträden, som leverantören med kundens uttryckliga samtycke får anlita för behandlingen av personuppgifter under avtalstiden. Leverantören har dock enligt punkt 3.4.1 alltid rätt att ersätta eller anlita nya underbiträden, men måste då enligt punkt 3.4.2 informera kunden om detta och invänta kundens eventuella synpunkter innan underbiträdet får påbörja sitt arbete. Om leverantören anlitar underbiträden behöver leverantören ingå ett skriftligt s.k. underbiträdesavtal med respektive underbiträde. Underbiträdesavtalet ska återspegla villkoren i Biträdesavtalet.