330.10 Information om personuppgiftsbiträdesavtalet 2018.1

Inledning

Nya regler om skydd av personuppgifter har införts genom dataskyddsförordningen GDPR. Reglerna är lag inom alla EUs medlemsländer från och med 25 maj 2018. Syftet bakom regelverket är att skapa ett enhetligt skydd av individers personuppgifter, och det medför även att alla register och lagring av personuppgifter på företag kommer att påverkas. I verksamheten på en redovisningsbyrå hanteras personuppgifter i anknytning till kundföretagen och detta kräver att ett särskilt avtal mellan byrån och uppdragsgivaren upprättas för att följa de nya reglerna. Srf konsulterna har därför tagit fram en sådan avtalsmall och en kort beskrivning av de olika punkterna lämnas enligt nedan.

Personuppgiftsbiträdesavtal

Det ska finnas ett skriftligt avtal mellan uppdragsgivaren och byrån för att reglera hur behandlingen av personuppgifter ska ske. Detta avtal har utformats som ett fristående avtal och det ska skrivas under av båda parter.

Srf konsulternas avtalsmall för personuppgiftsbiträdesavtal

Srf konsulternas avtalsmall är anpassad till verksamheten på en redovisningsbyrå. Det innebär i normalfallet att inga förändringar behöver göras mer än att komplettera mallen med namn på byrån samt på respektive uppdragsgivare, samt underskrifter. Översiktliga kommentarer avseende de olika delarna av mallen framgår enligt nedan.

Parter

Kundföretaget som är uppdragsgivare är den som förser byrån med personuppgifter och är därmed den som har huvudansvaret, vilket i regelverket kallas personuppgiftsansvarig. Fyll därför i respektive uppdragsgivares identitet som personuppgiftsansvarig.

Redovisningsbyrån behandlar de personuppgifter som man har erhållit enligt vad som har överens-kommits i uppdragsavtalet. Mallen ska därför fyllas i med redovisningsbyråns identitet som personuppgiftsbiträde.

Personuppgiftsansvarig

Uppdragsgivaren har huvudansvaret och ska bara förse byrån med de personuppgifter som är nödvändiga för uppdragets utförande. Om byrån skulle få uppgifter om personer som inte behövs för uppdragets utförande ska uppdragsgivaren kontaktas för att kunna återlämna dessa uppgifter.

Personuppgiftsbiträde

Redovisningsbyrån är den som behandlar de personuppgifter som erhållits av uppdragsgivaren. Enligt regelverket ingår även lagring i begreppet behandling, och den grundläggande principen enligt GDPR är att personuppgifter ska raderas eller återlämnas efter slutfört uppdrag eller på begäran av en registrerad person.

Av punkt 3c och 3d framgår att man även hänvisar till ”annan tillämplig lagstiftning”. GDPR är underställt viss annan lagstiftning som kan kräva att lagring sker även efter slutfört uppdrag. Detta kan t ex vara att lagra uppgifter för kundkännedom enligt lagen om åtgärder mot penningtvätt och finansiering av terrorism, eller kravet att bevara räkenskapsinformation enligt bokföringslagen.

Av punkt 3d framgår att lagringskrav kan finnas baserat på Rex (Svensk standard för redovisnings-uppdrag) som är plattform för uppdragsavtalen, och uttrycker en avtalad överenskommelse mellan parterna om att utföra vissa arbetsuppgifter enligt Rex. Detta utgör därmed rättslig grund, vilket påverkar rätten att lagra uppgifter, genom att uppdragsgivaren har avtalat en viss behandling samt därigenom även lämnat sitt samtycke till att byrån ska utföra dessa uppgifter.

Av punkt 3e framgår att byrån som är personuppgiftsbiträde även kan använda eventuella under-biträden, vilket t ex kan vara en annan byrå eller ett företag som tillhandahåller en molnbaserad tjänst som byrån utnyttjar för att utföra sitt uppdrag. Sådan användning av underbiträden ska godkännas av uppdragsgivaren, vilket kan ske generellt, och bekräftas genom punkt 3e.

Sekretess

Uppdragsgivarens sekretess framgår av uppdragsavtalet, och enligt biträdesavtalet regleras även att säkerhetsnivån för behandling av uppdragsgivarens tillhandahållna personuppgifter ska motsvara den säkerhetsnivå som finns hos uppdragsgivaren själv. Byrån måste därför informera sig om vilken typ av säkerhetsrutiner, brandväggar mm som finns hos uppdragsgivaren.

Rapportering

Om en incident inträffar som innebär att uppdragsgivarens personuppgifter kommer obehöriga till del ska byrån snarast möjligt informera till personuppgiftsansvarig, samt om incidenten är allvarlig anmäla till datainspektionen inom 72 timmar efter att den upptäckts.

Samverkan

En registrerad person som begär tillgång till sina uppgifter har rätt att få ut detta kostnadsfritt en gång per år från den som är personuppgiftsansvarig (uppdragsgivaren). Personuppgiftsbiträdet (byrån) ska vid sådan begäran bistå med att ta fram efterfrågad information. Notera särskilt att vissa uppgifter kan lyda under annan lagstiftning eller sekretess som måste beaktas.