Bäste medlem i Sveriges Tidskrifter,

Här nedan finner du en checklista som vägleder dig när du ska skriva personuppgiftsbiträdesavtal, något som kommer att krävas i samband med att den nya dataskyddsförordningen (GDPR) träder i kraft.

Personuppgiftsbiträdesavtal kommer du att behöva skriva med alla leverantörer som hanterar personuppgifter på uppdrag av dig/din organisation. Observera att detta inte är en mall. Varje företag har lite olika förutsättningar därför vore det riskfyllt av oss att göra färdiga avtal. Det skulle kunna innebära att vi vägleder våra medlemmar på ett felaktigt sätt.

Innehållet i checklistan utgår ifrån reglerna från dataskyddsförordningen och baseras på rättsläget den 15 februari.

Lagstiftningen på dataskyddsområdet inbegriper dataskyddsförordningen, tillämplig svensk dataskyddslag och speciallagstiftning på dataskyddsområdet.

Innehållet i checklistan utgör inte juridisk rådgivning och ersätter inte respektive medlems egna ansvar eller dataskyddsarbete.

Stockholm den 15 februari.

CHECKLISTA FÖR PERSONUPPGIFTSBITRÄDESAVTAL

1 INFÖR TRÄFFANDE AV AVTAL MED LEVERANTÖR

När ni ska anlita en leverantör (t.ex. en leverantör av ett IT-system, en producent av ett event, en distributör av en tidning, en konsultbyrå för ekonomifunktion) bör ni fundera över *om leverantören kommer att behandla personuppgifter för er räkning.* Ni måste då vara medvetna om att definitionerna av begreppen ”personuppgifter” och ”behandling” är mycket vida. Med *personuppgifter* menas varje upplysning som avser en identifierad eller identifierbar person och med *behandling* avses i princip allt man kan göra med personuppgifter såsom att samla in, lagra, använda, ändra, överföra och radera. Även ha tillgång till personuppgifter (t ex såsom kan vara fallet om en leverantör av underhålls- och supporttjänster loggar in i ett IT-system externt ifrån) räknas som en behandling av personuppgifter.

Om leverantören kommer att behandla personuppgifter för er räkning är leverantören ert *personuppgiftsbiträde* och ni är *personuppgiftsansvarig*. Ni

måste då se till att leverantören skyddar personuppgifterna och behandlar dem i enlighet med era instruktioner och med dataskyddsförordningen. För att kunna säkerställa det ska ni ingå ett skriftligt s.k. *personuppgiftsbiträdesavtal* som anger parternas rättigheter och skyldigheter och som sätter ramarna för personuppgiftsbehandlingen. Behandling av personuppgifter får inte påbörjas eller utföras av personuppgiftsbiträdet innan ett sådant avtal finns på plats mellan er.

Innan avtalet ingås ska ni undersöka om leverantören kan ge *tillräckliga garantier* för att denne kommer att vidta säkerhetsåtgärder för att skydda personuppgifterna så att behandlingen uppfyller kraven i dataskyddsförordningen. Utredningen bör omfatta en bedömning av leverantörens sakkunskap, tillförlitlighet och resurser.

Nedan finner ni en checklista som ni kan gå igenom för att se till att era avtal innehåller alla nödvändiga bestämmelser.

2 CHECKLISTA FÖR PERSONUPPGIFTSBITRÄDESAVTALET

När ett personuppgiftsbiträde utför behandling av personuppgifter för en personuppgiftsansvarigs räkning ska hanteringen regleras mellan parterna i ett skriftligt personuppgiftsbiträdesavtal.

Avtalet ska enligt dataskyddsförordningen särskilt innehålla följande:

☐ Föremålet för behandlingen och hur länge behandlingen ska pågå, samt dess art, ändamål och syfte. Det ska även framgå vilken typ av personuppgifter och vilka kategorier av registrerade som kommer att behandlas samt parternas rättigheter och skyldigheter.

I avtalet ska det finnas en beskrivning av vad personuppgiftsbiträdet ska göra för den personuppgiftsansvariges räkning och varför. Denna beskrivning kan ingå som en bakgrund till avtalet samt ingå i de instruktioner för behandlingen som den personuppgiftsansvarige ska lämna till personuppgiftsbiträdet (se nedan).

☐ Ett krav på att personuppgiftsbiträdets behandling endast får utföras i enlighet med instruktioner från den personuppgiftsansvarige.

För att personuppgiftsbiträdet ska kunna följa era instruktioner bör personuppgiftsbiträdesavtalet innehålla en specifikation över era instruktioner för den behandling personuppgiftsbiträdet ska utföra. Instruktionerna bör bl.a. innehålla en beskrivning av ändamålet, dvs. varför leverantören ska behandla personuppgifter för er räkning, vilka personuppgifter och behandlingsaktiviteter det rör sig om, var behandlingen kommer att äga rum och vilka säkerhetsåtgärder som leverantören ska vidta. I avtalet ska även framgå att varje person som är behörig att utföra arbeta åt personuppgiftsbiträdet ska förbinda sig att endast behandla personuppgifterna enligt instruktionerna.

☐ Personuppgiftsbiträdets skyldighet att se till att det, efter den personuppgiftsansvariges godkännande, finns förutsättningar för att överföra personuppgifter till tredjeland.

Avtalet ska innehålla bestämmelse om att personuppgiftsbiträdet endast får överföra personuppgifter till ett s.k. tredjeland, dvs. ett land utanför EU/EES, med den personuppgiftsansvariges godkännande. Som huvudregel är sådan överföring förbjuden om inte EU-kommissionen har beslutat att landet säkerställer en tillräcklig skyddsnivå för personuppgifter. Kommissionen har fattat sådana beslut för exempelvis Schweiz, Argentina och Nya Zeeland. Utan ett sådant beslut får överföringar endast utföras undantagsvis efter att lämpliga skyddsåtgärder vidtagits. Sådana skyddsåtgärder kan t.ex. vara att parterna avtalat om att tillämpa kommissionens standardavtalsklausuler eller att man inom koncernen antagit bindande företagsbestämmelser för överföringar till tredjeländer, s.k. BCR. Om personuppgiftsbiträdet har fått godkännande från den personuppgiftsansvarige att överföra uppgifter till tredjeland ska biträdet se till att det finns laglig grund för sådan överföring.

☐ Ett krav om att alla personer som behandlar personuppgifterna har åtagit sig att iaktta konfidentialitet eller är under lagstadgad tystnadsplikt. samt

I avtalet ska det föreskrivas att personuppgiftsbiträdet ska säkerställa att endast sådan personal som måste ha tillgång till uppgifterna har sådan tillgång samt att den personal som ges tillgång har instruerats om hur behandlingen ska gå till och är bundna av sekretess eller tystnadsplikt.

☐ Att personuppgiftsbiträdet inte utan godkännande från den personuppgiftsansvarige får lämna ut eller tillgängliggöra personuppgifterna till tredje part.

Avtalet ska föreskriva att personuppgiftsbiträdet inte har rätt att utan föregående skriftligt godkännande från den personuppgiftsansvarige lämna ut eller på annat sätt tillgängliggöra uppgifter som rör behandlingen av personuppgifter under personuppgiftsbiträdesavtalet till tredje parter såsom tillsynsmyndigheter, registrerade eller andra företag eller organisationer.

☐ Krav på att personuppgiftsbiträdet genomför lämpliga tekniska och organisatoriska åtgärder som tillförsäkrar en hög nivå av säkerhet.

Avtalet ska föreskriva att personuppgiftsbiträdet är skyldigt att vidta säkerhetsåtgärder för att skydda personuppgifterna. Dessa åtgärder kan vara av både teknisk och organisatorisk karaktär och kan exempelvis bestå av pseudonymisering, kryptering, behörighetskontroller, regelbundna test av system och incidenthantering. De säkerhetsåtgärder som vidtas ska vara anpassade till de risker som behandlingen medför.

☐ Förutsättningarna för att personuppgiftsbiträdet ska kunna anlita underleverantörer som behandlar personuppgifterna.

Personuppgiftsbiträdet får inte anlita underbiträden som behandlar de personuppgifter som den personuppgiftsansvarige lämnat ut utan föregående skriftligt godkännande från den personuppgiftsansvarige. Om personuppgiftsbiträdet har fått ett generellt godkännande från den personuppgiftsansvarige att anlita underbiträden ska biträdet informera den personuppgiftsansvarige när biträdet planerar att anlita ett nytt underbiträde. Alla underbiträden som anlitas ska vara bundna av samma skyldigheter som personuppgiftsbiträdet är enligt personuppgiftsbiträdesavtalet.

☐ Personuppgiftsbiträdets skyldigheter att bistå den personuppgiftsansvarige att uppfylla sina skyldigheter.

Avtalet ska föreskriva att personuppgiftsbiträdet ska hjälpa den personuppgiftsansvarige att besvara begäran från de registrerade om att utöva dessas rättigheter, såsom rätt till tillgång, rättelse, radering och dataportabilitet. Personuppgiftbiträdet ska även bistå den personuppgiftsansvarige med att vidta lämpliga säkerhetsåtgärder, lämna den information som behövs för att anmäla personuppgiftsincidenter till tillsynsmyndigheter och registrerade samt utföra konsekvensbedömningar och förhandssamråd.

☐ Möjligheterna för den personuppgiftsansvarige att granska personuppgiftsbiträdet för att säkerställa att denne uppfyller sina skyldigheter gentemot den personuppgiftsansvarige.

Avtalet ska föreskriva att personuppgiftsbiträdet på begäran ska lämna tillräcklig information till den personuppgiftsansvarige så att denne kan granska att personuppgiftsbiträdet utför sina skyldigheter enligt avtalet och dataskyddsförordningen.

☐ Personuppgiftsbiträdets skyldigheter efter det att behandlingen upphör.

Avtalet ska föreskriva att personuppgiftsbiträdet efter avslutad behandling är skyldig att antingen permanent radera eller återlämna personuppgifterna till den personuppgiftsansvarige, samt radera eventuella kopior.

Avtalet bör lämpligen även innehålla följande beståndsdelar och bestämmelser även om dessa inte är krav enligt dataskyddsförordningen:

☐ Uppgift om parternas identitet samt datum och beskrivning av varför avtalet ingås.

Det är viktigt att vara tydlig med vilka parter som ingår personuppgiftsbiträdesavtalet. Parternas namn och organisationsnummer bör därför tydligt framgå och avtalet bör vara daterat så att det är lätt att hänvisa till. Med fördel ger ni även en kortfattad bakgrund till varför parterna ingår personuppgiftsbiträdesavtalet.

☐ Om personuppgiftsbiträdet ska ha rätt till någon ersättning för det arbete som denne utför med anledning av personuppgiftsbiträdesavtalet.

För personuppgiftsbiträdet kan skyldigheterna enligt personuppgiftsbiträdesavtalet vara betungande och ta mycket resurser i anspråk. Personuppgiftsbiträdet kommer därför att önska ersättning för sådant som går utöver dennes skyldigheter enligt dataskyddsförordningen.

☐ Hur ansvaret ska fördelas för skadestånd till de registrerade, administrativa sanktionsavgifter och övriga skador.

En av de stora nyheterna i dataskyddsförordningen är att överträdelser förenas med stora sanktionsavgifter. Dessutom kan registrerade vars uppgifter behandlats felaktigt kräva skadestånd. I avtalet bör parterna reglera hur ansvaret ska fördelas. Lämpligen bör inte parterna sträva efter att skjuta över hela ansvaret på motparten utan istället komma överens om en fördelning som baseras på respektive parts skuld till överträdelsen.

☐ Hur ändringar i personuppgiftsbiträdesavtalet kan göras.

Den personuppgiftsansvarige är ytterst ansvarig för behandlingen av personuppgifterna. Det är därför viktigt att det finns en möjlighet för den personuppgiftsansvarige att kunna göra ändringar i avtalet om det krävs för att uppfylla dataskyddsförordningen eller annan tillämplig lagstiftning. Det är särskilt viktigt eftersom många delar av dataskyddsförordningen ännu är oklara hur de ska fungera i praktiken.

☐ Bestämmelse om tillämplig lag och tvistelösning.

Det bör anges vad som händer vid tvist. Om detta regleras i huvudavtalet kan man införa en hänvisning till dessa bestämmelser. I annat fall kan det vara bra att skriva att tolkning och tillämpning av avtalet ska ske i enlighet med svensk rätt och att tvist ska lösas av domstol alternativt skiljnämnd i Sverige.

☐ Bestämmelse om avtalstid.

Avtalet bör gälla så länge som personuppgiftsbiträdet behandlar personuppgifter för den personuppgiftsansvariges räkning.

☐ Vilken rättslig ställning personuppgiftsbiträdesavtalet har.

Personuppgiftsbiträdesavtalet kan ingå som en bilaga till huvudavtalet om tjänsteleverans som ni ingår med leverantören eller fungera som ett fristående avtal. Om det förekommer motstridiga uppgifter i huvudavtalet och personuppgiftsbiträdesavtalet bör det anges vilket som ska äga företräde.

☐ Signaturer.

Om personuppgiftsbiträdesavtalet ingår som en bilaga till huvudavtalet behövs inte signaturer eftersom det görs på huvudavtalet. Om personuppgiftsbiträdesavtalet däremot är fristående behövs signaturer.