Delphi

Checklista personuppgifts-biträdesavtal

När personuppgifter behandlas på uppdrag av en annan aktör föreligger enligt GDPR en relation mellan en personuppgiftsansvarig och ett personuppgiftsbiträde. I en sådan relation ska enligt artikel 28 i GDPR ett personuppgiftsbiträdesavtal eller ”annan rättsakt” upprättas. Det finns alltså inte ett absolut krav på att ett avtal upprättas, men det är det vanligaste. Enligt bestämmelsen finns flera krav på vad som ska ingå i ett sådant avtal/rättsakt.

Här följer en checklista på vad som är relevant att identifiera i ett personuppgiftsbiträdesavtal för att se till att det uppfyller GDPR:s krav.

Avtal mellan [Kund] och [Leverantör] om [Vad gäller avtalet?]

Uppfyller leverantören generella krav på att behandla personuppgifter för kundens räkning?

Leverantören måste ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder så att behandlingen uppfyller GDPR:s krav. I praktiken innebär detta krav att kunden inte bör anlita leverantörer där kunden vet/misstänker att kraven på säkerhet inte kommer att kunna uppfyllas. Detta krav är i praktiken inte något problem t.ex. avseende etablerade molntjänstleverantörer.

☐ Uppfyllt

Information om behandlingen

Kontrollera så att det i avtalet framgår:

☐ Föremålet för behandlingen

☐ Hur länge uppgifterna kommer behandlas

☐ Behandlingens art

☐ Behandlingens ändamål

☐ Typer av personuppgifter som behandlas

☐ Kategorier av registrerade vars uppgifter behandlas

Denna information står ofta i en bilaga till biträdesavtalet, men kan även anges i själva.

Den personuppgiftsansvariges instruktioner

Kontrollera så att det av avtalet framgår:

☐ att personuppgiftsbiträdet endast får behandla personer på kundens instruktioner, som också måste dokumenteras. Sådana instruktioner kan bland annat upprättas separat, framgå av personuppgiftsbiträdesavtalet eller det huvudavtal som personuppgiftsbiträdesavtalet är kopplat till.

Kontrollera:

☐ om undantag finns för situationer när annan behandling än enligt instruktionerna måste ske på grund av bestämmelser enligt EU-rätten eller nationell rätt som personuppgiftsbiträdet omfattas av. Finns ett sådant undantag, ska det framgå att personuppgiftsbiträdet ska informera kunden om sådan behandling om så inte är förbjudet.

Sekretess och tystnadsplikt

Kontrollera:

☐ om det framgår av personuppgiftsbiträdesavtalet att de personer som behandlar personuppgifter omfattas av sekretess eller lämplig tystnadsplikt.

Tekniska och organisatoriska åtgärder

Kontrollera:

☐ om det i avtalet framgår att personuppgiftsbiträdet ska vidta tekniska och organisatoriska åtgärder för att skydda personuppgifter. Säkerställ att konkreta åtgärder nämns, snarare än endast en generell skrivning om att sådana åtgärder ska vidtas. Exempel på åtgärder kan vara att personuppgifter krypteras, att IT-systems säkerhet testas och att backuper av personuppgifter finns.

Anlitande av underbiträden

Kontrollera:

☐ om det regleras i avtalet hur personuppgiftsbiträdet får anlita underbiträden. Det måste antingen ske genom ett generellt tillstånd från kunden, eller genom att kunden godkänner anlitandet av underbiträden i varje enskilt fall. Om ett generellt tillstånd har lämnats, måste det framgå av avtalet att personuppgiftsbiträdet lämnar information till kunden varje gång ett nytt underbiträde planeras anlitas. Detta för att ge kunden möjligheten att invända mot anlitande av nya underbiträden.

Kontrollera:

☐ att det i personuppgiftsbiträdesavtalet regleras att samma skyldigheter måste ställas på eventuella underbiträden som på personuppgiftsbiträdet själv

☐ att det i personuppgiftsbiträdesavtalet regleras att personuppgiftsbiträdet ska vara fullt ansvarig för sina underbiträden om de inte fullgör sina skyldigheter.

Hjälp med begäran om registrerades rättigheter

Kontrollera:

- ☐ att det i avtalet regleras att personuppgiftsbiträdet ska vidta tekniska och organisatoriska åtgärder för att hjälpa kunden att hantera förfrågningar från registrerade avseende deras rättigheter enligt kapitel III i GDPR (exempelvis rätt till registerutdrag/tillgång, radering och rättelse).

Hjälp med skyldigheter enligt artikel 32-36

Kontrollera:

- ☐ att det i avtalet regleras att personuppgiftsbiträdet ska hjälpa kunden med kundens skyldigheter
  - ☐ i samband med säkerhet (brukar ofta saknas)
  - ☐ vid personuppgiftsincidenter
  - ☐ vid konsekvensbedömningar och förhandssamråd i den utsträckning som är lämpligt.

Radering eller återlämnande av personuppgifter

Framgår det av avtalet:

- ☐ att kunden har en rätt att begära att uppgifterna antingen raderas eller återlämnas av personuppgiftsbiträdet när behandlingen/avtalsförhållandet upphört?
- ☐ att personuppgiftsbiträdet ska radera eventuella kopior (saknas ibland)?

Tillgång till information och rätt till granskning

Kontrollera:

- ☐ att det i avtalet finns en skyldighet för personuppgiftsbiträdet att ge kunden tillgång till information som visar att biträdet uppfyller sina skyldigheter
- ☐ att kunden har en rätt att utföra granskningar, inklusive inspektioner, av biträdets personuppgiftsbehandling, utan att några långtgående begränsningar i denna rätt ställs upp.

Kommersiella aspekter på avtalet (ej GDPR-krav)

Finns det några ansvarsbegränsningar gällande skadestånd i avtalet? Finns sådana ansvarsbegränsningar även gällande administrativa sanktionsavgifter enligt GDPR?

Ska kunden betala ersättning till personuppgiftsbiträdet i några situationer när biträdet uppfyller sina skyldigheter i enlighet med punkterna ovan?