## Checklista för bedömning av externt biträdesavtal

Det måste finnas ett skriftligt biträdesavtal. I det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i (enligt art 28 i Dataskyddsförordningen).

*Uppfyllt? [Ja / nej]*

**Följande punkter ska framgå av biträdesavtalet:**

. Framgår att biträdet är skyldigt att tillämpa Dataskyddsförordningen och i övrigt Svensk lagstiftning när det gäller behandling av de personuppgifter som omfattas av avtalet.
*Uppfyllt? [Ja / nej]*

. Framgår föremålet för behandlingen (vad det är för personuppgifter som ska behandlas, vilka kategorier av registrerade som återfinns) (jmfr art 28 p 3 i Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. Framgår om det är särskilt känsliga personuppgifter (ingår känsliga personuppgifter (definierat i lagstiftning art 9 p 1 Dataskyddsförordningen) eller extra skyddsvärda (som av sitt sammanhang eller sin karaktär är extra skyddsvärda) (jmfr art 28 p 3 i Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. Framgår behandlingens varaktighet (tidsbestämt eller tills vidare) (jmfr art 28 p 3 i Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. framgår att personuppgiftsbiträdet är skyldigt att vidta lämpliga säkerhetsåtgärder (enligt art 32 i Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. framgår att personuppgiftsbiträdet endast får behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner och därmed säkerställa att personuppgiftsbiträdet inte behandlar personuppgifter för andra ändamål än dem som personuppgiftsbiträdet anlitats för (Art 29 Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. framgår att personuppgiftsbiträdet endast får överföra personuppgifter till ett land som ligger utanför EU och som saknar tillräckligt legala skydd för hanteringen av personuppgifter (s.k. tredje land) om det finns uttryckliga instruktioner om detta från personuppgiftsansvarig. (Art 28 p 3 a, Dataskyddsförordningen) *Uppfyllt? [Ja / nej]*

. säkerställa att den personuppgiftsansvarige notifieras innan underbiträden anlitas (underbiträden till personuppgiftsbiträdes som kan komma att behandla den personuppgiftsansvariges personuppgifter) (enligt art 28 p 3 d, Dataskyddsförordningen). Observera att det inte är någon självklarhet att underbiträden ska utnyttjas. Den personuppgiftsansvarige kan mycket väl villkora att inga underbiträden ska finnas. Om inget skrivs om det i avtalet så finns det inte någon rätt att anlita underbiträden (enligt art 28 p 1 Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. säkerställa att de eventuella underbiträden som avses ovan villkoras med samma skyldigheter som personuppgiftsbiträdet har (enligt art 28 p 4, Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. säkerställa att den personuppgiftsansvarige på lämpligt sätt har möjlighet att följa upp att personuppgiftsbiträden lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen vidtar lämpliga säkerhetsåtgärder, t.ex. genom möjlighet till revision. (enligt art 28 p 3 c, Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet (avtal om tystnadsplikt) eller omfattas av en lämplig lagstadgad tystnadsplikt, (Art 28 p 3 b, Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstankar om att någon hos den personuppgiftsansvarige eller hos något personuppgiftsbiträde haft obehörig åtkomst till personuppgifterna
*Uppfyllt? [Ja / nej]*

. villkor om att biträdet ska understödja den personuppgiftsansvarige med det som behövs för att tekniskt möjliggöra att den personuppgiftsansvarige hanterar de registrerades rättigheter (som t.ex. registerutdrag, radering av personuppgifter, rättelse m.m.), (Art 28 p 3 e, Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. personuppgiftsbiträdet ska notifiera Region Skåne snarast vid händelse av personuppgiftincident. Samt i övrigt stödjer den personuppgiftsansvarige med anmälan av en personuppgiftsincident till tillsynsmyndigheten samt i förekommande fall till registrerade. (art 28 p 3 f, Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*

. Ansvar för skada / skadeståndsbegränsning. Finns bestämmelser i avtal om hur krav på ersättning för skada (eller om en behörig myndighet utfärdar vite eller andra administrativa påföljder) med anledning av personuppgiftsbehandling? I Region Skånes standardavtal står att om personuppgiftsbiträde gör något i strid med instruktioner, detta avtal eller gällande dataskyddsregler ska personuppgiftsbiträde hålla personuppgiftsansvarig skadeslös. [ytterst är skadeståndsbegräsningar en förhandlingsfråga, men det är för personuppgiftsansvarig viktigt att det är tydligt vad som gäller om biträdet bryter mot de krav som ställts i avtalet. Eftersom både personuppgiftsansvarig och personuppgiftsbiträde har ansvar enigt Dataskyddsförordningen så kan skadestånd från registrerad riktas mot vilken som helst av parterna. Finns den tydlighet i avtalet kring skadeståndsansvar blir det lättare att rikta regresskrav mot motparten (alltså att personuppgiftsansvarig, efter att denne betalt skadestånd till registrerad kan rikta krav mot personuppgiftsbiträdet som varit den som gjort något otillåtet) ]
*Uppfyllt? [Ja / nej]*

. säkerställa att parterna vet vilka åtgärder (raderande eller återlämning till personuppgiftsansvarig) som ska vidtas vid avtalets upphörande så att personuppgiftsbiträdet inte har åtkomst till personuppgifterna därefter. (Art 28 p 3 g, Dataskyddsförordningen)
*Uppfyllt? [Ja / nej]*