



1. Bedömning av personuppgiftsbiträdesavtal

Checklistan nedan kan användas för att bedöma om ett personuppgiftsbiträdesavtal (PUB-avtal) innehåller vad ett sådant avtal ska innehålla enligt EU:s dataskyddsförordning.

1.1 Checklista

Krav	Ev. kommentar	Är kravet uppfyllt?	
Avtalets form			
Finns det ett skriftligt avtal?	Det måste finnas ett skriftligt biträdesavtal (se artikel 28 i Dataskyddsförordningen).	Ja	Nej
Skyldighet att följa gällande lagstiftning			
Framgår att biträdet är skyldigt att tillämpa Dataskyddsförordningen och i övrigt svensk lagstiftning när det gäller behandling av de personuppgifter som omfattas av avtalet?		Ja	Nej
Föremålet för behandlingen			
Framgår föremålet för behandlingen, dvs. vad det är för typ av personuppgifter som ska behandlas, vilka kategorier av registrerade berörs etc.?	Se artikel 28 punkten 3 i Dataskyddsförordningen.	Ja	Nej
Framgår om det är särskilt känsliga personuppgifter eller extra skyddsvärda personuppgifter som kommer att ingå i behandlingen?	Känsliga personuppgifter (även kallade särskilda kategorier av personuppgifter) är personuppgifter som avser hälsa, sexualliv, biometriska uppgifter, ras/etniskt ursprung, politiska åsikter, religiös/filosofisk	Ja	Nej

	övertygelse eller medlemskap i fackförening. Personuppgifter kan också vara extra skyddsvärda, t.ex. personnummer eller uppgifter som omfattas av sekretess.		
Behandlingens varaktighet			
Framgår hur länge behandlingen ska pågå?	Behandlingstiden kan antingen tidsbestämmas eller gälla tills vidare.	Ja	Nej
Instruktioner och säkerhetsåtgärder			
Framgår det att personuppgiftsbiträdet är skyldigt att vidta lämpliga säkerhetsåtgärder?	Se artikel 32 i Dataskyddsförordningen.	Ja	Nej
Framgår det att personuppgiftsbiträdet endast får behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner?	Genom en sådan bestämmelse säkerställs att personuppgiftsbiträdet inte behandlar personuppgifter för andra ändamål än dem som personuppgiftsbiträdet har anlitats för. Se artikel 29 i Dataskyddsförordningen	Ja	Nej
Finns sådana instruktioner, t.ex. i en bilaga till PUB-avtalet?	Man får beakta att det ofta är biträdet som kommer att författa instruktionerna utifrån att det är biträdet som känner till sin tjänst bäst. Instruktionerna bör därför granskas noga så de överensstämmer med den personuppgiftsansvariges intention.	Ja	Nej
Är instruktionerna tillräckliga för att säkerställa en lämplig skyddsnivå för de aktuella personuppgifterna?		Ja	Nej



Överföring till land utanför EU			
Framgår det att personuppgiftsbiträdet endast får överföra personuppgifter till ett land som ligger utanför EU (s.k. tredje land) om det finns uttryckliga instruktioner om detta från personuppgiftsansvarig?	Se artikel 28 punkten 3 a i Dataskyddsförordningen	Ja	Nej
Om sådan överföring tillåts; finns det instruktioner som anger vilka förutsättningar som ska vara uppfyllda för att överföringen ska få genomföras?	Exempelvis bör anges att sådan överföring endast får ske om förutsättningarna i artikel 45-47 i Dataskyddsförordningen är uppfyllda.	Ja	Nej
Underbiträden (underleverantörer)			
Säkerställs att den personuppgiftsansvarige notifieras innan underbiträden/underleverantörer som kan komma att behandla den personuppgiftsansvariges personuppgifter anlitas?	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 punkten 1 i Dataskyddsförordningen)	Ja	Nej
Förbinder sig biträdet att se till att de eventuella underbiträden/underleverantörer som personuppgiftsbiträdet anlitar åläggs samma skyldigheter i fråga om dataskydd som de som personuppgiftsbiträdet har i avtalet med oss?	Underbiträdet måste åläggas dessa skyldigheter i ett skriftligt avtal.	Ja	Nej



Uppföljning och revision			
Säkerställs att den personuppgiftsansvarige på lämpligt sätt har möjlighet att följa upp att personuppgiftsbiträdet lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen vidtar lämpliga säkerhetsåtgärder, t.ex. genom möjlighet till revision?	Fundera på vilken typ av information som krävs för att vi ska kunna följa upp och bedöma om biträdet sköter sig. Kan exempelvis årliga rapporter eller kopior på rapporter från internrevisioner vara tillräckligt? Kan detta vara tillräckligt i kombination med möjlighet till revision på plats vid misstanke om misskötsamhet?	Ja	Nej
Säkerställs 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?	Fundera över vilka funktioner som redan finns inbyggda i tjänsten, t.ex. loggar? Ger avtalet oss möjlighet att begära in ytterligare information eller rätt till att granska på plats?	Ja	Nej
Konfidentialitet och tystnadsplikt			
Säkerställs att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet (t.ex. genom avtal om tystnadsplikt) eller omfattas av en lämplig lagstadgad tystnadsplikt?	Säkerställs oftast genom att en sekretessbestämmelse tas in i avtalet.	Ja	Nej
De registrerades rättigheter			
Finns det villkor om att biträdet ska understödja den personuppgiftsansvarige med det som behövs rent tekniskt för att möjliggöra att den personuppgiftsansvarige kan tillgodose de registrerades rättigheter?	Vi måste via inbyggda funktioner i verktyget eller genom annan hjälp från leverantören kunna se till att vi kan tillgodose enskilda personers rättigheter enligt GDPR som exempelvis rätten till registerutdrag, radering och rättelse av personuppgifter. Se artikel 15-21 i Dataskyddsförordningen.	Ja	Nej



Personuppgiftsincidenter			
Anges att personuppgiftsbiträdet ska notifiera personuppgiftsansvarig utan onödigt dröjsmål vid händelse av personuppgiftsincident?	Se artikel 33.2 i Dataskyddsförordningen	Ja	Nej
Finns det krav på att biträdet även i övrigt ska stödja den personuppgiftsansvarige vid anmälan av en personuppgiftsincident till tillsynsmyndigheten samt i förekommande fall med att ge information till registrerade?	Detta krav uppfylls exempelvis genom att biträdet förbinder sig att ge oss all information om vad som har hänt, medverka vid utredning av incidenten och att svara på våra frågor.	Ja	Nej
Ansvar för skada/skadeståndsbegränsning.			
Finns bestämmelser i avtalet om hur krav på ersättning för skada (eller om en behörig myndighet utfärdar vite eller andra administrativa påföljder) med anledning av personuppgiftsbehandling ska hanteras?	Ytterst är skadeståndsbegränsningar 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 biträde har ansvar enligt Dataskyddsförordningen så kan skadestånd från registrerad riktas mot vilken som helst av parterna. Finns det en 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 biträdet som varit den som gjort något otillåtet). Många avtal hänvisar till att ansvarsfördelning ska ske enligt artikel 82 i Dataskyddsförordningen. Det innebär att personuppgiftsansvarig som huvudregel är ansvarig och att biträdet endast är ansvarigt om det kan visas att de agerat i strid med instruktioner från personuppgiftsansvarig. Det är därför av stor vikt att instruktionerna är korrekt beskrivna.	Ja	Nej



Vad händer vid avtalets upphörande?			
Regleras vilka åtgärder (raderande eller återlämning till personuppgiftsansvarig) som ska vidtas vid avtalets upphörande?	Detta är viktigt så att personuppgiftsbiträdet inte fortsätter att ha åtkomst till personuppgifterna efter att avtalet har upphört.	Ja	Nej

1.2 Särskilt om sekretess

Om de uppgifter som ska hanteras av personuppgiftsbiträdet omfattas av Offentlighet- och sekretesslagen (2009:400) (OSL), ställer detta särskilda krav på hur en leverantör får hantera uppgifterna.

De närmare kraven ska konkretiseras genom att en riskanalys genomförs där åtgärder för att hantera dessa risker identifieras. Dessa krav bör sedan inkluderas i avtal med leverantören, antingen som en del av huvudavtalet, som del av ett personuppgiftsbiträdesavtal eller som ett särskilt sekretessavtal.

Här ska understrykas att denna fråga är komplex och svår att hantera. En särskild problematik när det gäller OSL är att uppgifterna inte otillåtet får röjas, ens för ett biträde. Redan genom att uppgifterna överlämnas till en leverantör kan innebära att uppgifterna anses vara röjda, något som är förbjudet enligt lag. För att motverka att uppgifterna ska anses vara röjda kan åtgärder vidtas som gör det mer eller mindre sannolikt att leverantören faktiskt tar del av uppgifterna, exempelvis genom tekniska lösningar och/eller avtalsregleringar.
