CHECKLISTA –

kan användas vid upprättande eller granskning av personbiträdesavtal GDPR

Nedan finns en checklista som kan användas av personuppgiftsansvariga (PuA) dels när de ska upprätta ett personbiträdesavtal och dels när ett avtal som upprättas av ett personuppgiftsbiträde (PuB) ska granskas.

Avtalspunkt	**Kommentar**	**Artikel i GDPR**
Parter	PuA – controller och PuB - processor	
Föremålet för behandlingen (art och innehåll)	Ändamålsbeskrivning av är PUB – roll, system, utskrifter	jfr 28.3 GDPR samt skäl 81
Behandlingens varaktighet	Tidsbestämt eller tillsvidare	jfr 28.3 GDPR,
Typen av personuppgifter	Känsliga eller extra skyddsvärda	jfr 28.3 GDPR,
kategorier av registrerade	Vems uppgifter, anställda, kunder, medlemmar	jfr 28.3 GDPR,
PUA:s skyldigheter		
Hänvisning till tillräckliga garantier	Hur ska PuB visa sin förmåga -”accountability” eller ”privacy by design”	jfr 28.1 och 28.3 h) GDPR
Underleverantörer	Krävs – förhandstillstånd innan underbiträden anlitas. Om PUA gör invändningar – bryts avtalet. Ev. ekonomisk ersättning.	jfr 28.2, 28.3 d) och 28.4 GDPR,
Bilaga med ev. underleverantörer och deras ev. underleverantörer,	Organisation, adress, uppgift i kedjan	jfr 28.2, 28.3 d) och 28.4 GDPR,
Tredje land	Krav på lokalisering av data – åtkomst på distans för service, support m.m.	

	PuB ska informera om de får krav på att lämna ut information (NSA eller andra myndigheter)	jfr 28.3 a) GDPR,
Dokumenterade instruktioner (ev. bilaga)	Vad ska PuB göra – teknikkrav T.ex. krypterad kommunikation	jfr 28.3 a) GDPR,
Sekretess/konfidentialitet	PuB ska tystnadsplikt – betr. all information	jfr 28.3 b) GDPR,
Säkerhetsåtgärder	Specificerade krav	jfr 28.3 c) GDPR,
Hjälpa PUA att fullgöra sina skyldigheter	Specificerat, t.ex. hjälp med information till registerutdrag	jfr 28.3 e) och f) GDPR,
Personuppgiftsincident	Specificera - PuB ska informera PuA skriftligt om incident inom 36 timmar från att denne fått vetskap, incidentens art, hur många som drabbats, DSO kontaktuppgifter, konsekvenser, vidtagna åtgärder m.m.	Jfr 33.2 GDPR
Upphörande av behandling vid avtalsslut	Specificera – tidsfrister för t.ex. radering m.m.	jfr 28.3 g) GDPR,
Revision	Specificera - hur ska revision göras och vad ska denna visa samt hur ska resultatet redovisas	jfr 28.3 h) GDPR,
Ansvar för skada	Krav på försäkring. Riktas krav på ersättning för skada (eller om en behörig myndighet utfärdar vite eller andra administrativa påföljder) med anledning av personuppgiftsbehandling i strid med instruktioner, detta avtal eller gällande dataskyddsregler ska PuB hålla PuA skadeslös.	
Åtgärd vid om PuB anser behandlingen är olaglig	Specificera – Vad som bör göras, t.ex. vem beslutar att behandlingen ska stoppas.	jfr 28.3 andra st GDPR,
Avtalsperiod		
Tvistelösningar	Lagval och i vilken domstol ska tvister avgöras.	