Schoolsoft

Vindelns Kommun

Checklista Sida 1(4)
Datum
2018-05-02

Antagen av kommunledningsgruppen den 2 maj 2018

Checklista för granskning av personuppgiftsbiträdesavtal

Sammanfattning

Denna checklista är framtagen av Sveriges kommuner och Landsting (SKL) och ska användas av personuppgiftsansvariga (PuA) i Vindelns kommun för att granska förslag till personuppgiftsbiträdesavtal som upprättats av ett personuppgiftsbiträde (PuB).

Samtliga avtalspunkter i checklistan ska finnas med i biträdesavtalet för att det ska godkännas.

Definitioner

Personuppgiftsansvarig (PuA):	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. I vårt fall är respektive nämnd som är personuppgiftsansvarig för sina verksamheter och system.
Personuppgiftsbiträde (PuB):	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Dataskyddsombud (DSO):	Dataskyddsombudet ska övervaka att organisationen följer dataskyddsförordningen. Det innebär bland annat att samla in information om hur organisationen behandlar personuppgifter, kontrollera att organisationen följer bestämmelser och interna styrdokument samt informera och ge råd inom organisationen.

Vindelns kommun
922 81 Vindeln
Besöksadress:
Kommunalhusvägen 11
Växel:
0933-140 00
Fax:
0933-140 03
vindelns.kommun@vindeln.se
www.vindeln.se

Vindelns Kommun

Checklista

[redacted]	Uppgiften finns med
Delvis	Uppgiften finns med men ändringar eller kompletteringar behöver göras
[redacted]	Uppgiften finns inte med, avtalet behöver uppdateras med mer information

Avtalspunkt	Kommentar	Artikel i GDPR	Finns uppgiften med? Ja, delvis eller nej? Beskriv vad som saknas
Parter och kontaktinformation	PuA (nämnd, styrelse eller bolag) och BuB. Kontaktuppgifter		Ja
Föremålet för behandlingen (art och innehåll)	Ändamålsbeskrivning av PUB – roll, system, utskrifter	jfr 28.3 GDPR samt skäl 81	1
Behandlingens varaktighet	Tidsbestämt eller tillsvidare	jfr 28.3 GDPR	11
Typen av personuppgifter	känslig eller extra skyddsvärd	jfr 28.3 GDPR	5 Bil 1
Kategorier av registrerade	t.ex. anställda, medborgare, brukare, privatpersoner	jfr 28.3 GDPR	5
PuA:s skyldigheter	Vad vi ska ansvara för		3
Hänvisning till tillräckliga garantier	Hur ska PuB visa sin förmåga att ge tillräckliga tekniska och organisatoriska skyddsåtgärder samt inbyggda skyddsmekanismer	jfr 28.1 och 28.3 h) GDPR	4 Bil 1
Underleverantörer	Anges det att det krävs tillstånd innan underbiträden får anlitas? Om PuA gör invändningar, bryts avtalet eller lämnas ekonomisk ersättning?	jfr 28.2, 28.3 d) och 28.4 GDPR	6 10
Bilaga med eventuella underleverantörer och deras eventuella underleverantörer	Organisation, adress samt vilken uppgift underleverantören har och hur mycket av information som den kan ta del av	jfr 28.2, 28.3 d) och 28.4 GDPR	Bil Kontakt uppgift saknas.
Ansvar för att säkerställa att underleverantören uppfyller samma krav	Underleverantören ska uppfylla samma krav som huvudleverantören ha åtagits sig		6:2

som i PuB-avtalet mellan PuA och PuB	i avtal.		

Avtalspunkt	Kommentar	Artikel i GDPR	Finns uppgiften med? Ja, delvis eller nej? Beskriv vad som saknas
Tredje land	Krav på lokalisering av data – åtkomst på distans via service, support med mera. PuB ska informera om de får krav på att lämna ut information (NSA eller andra myndigheter)	jfr 28.3 a) GDPR	7 Bil 1
Dokumenterande instruktioner (eventuell bilaga)	Vad ska PuB göra – teknikkrav T.ex. krypterad kommunikation	jfr 28.3 a) GDPR	8a
Sekretess/konfidentialitet	PuB ska ha tystnadsplikt beträffande all information	jfr 28.3 b) GDPR	9
Säkerhetsåtgärder	Specificerade krav	jfr 28.3 c) GDPR	9
Hjälpa PUA att fullgöra sina skyldigheter	Specificerat, t.ex. hjälp med information till registerutdrag	jfr 28.3 e) och f) GDPR	5:3
Om serviceavtal finns	Servicenivå, vilka krav har ställts och uppfyller det våra krav?		—
Personuppgiftsincident	Specificera att PuB skyndsamt ska informera PuA skriftligt när denne fått vetskap om incidentens art, hur många som drabbats, konsekvenser och vidtagna åtgärder m.m. Information ska även finnas om kontaktuppgifter till DSO.	Jfr 33.2 GDPR	5:7
Upphörande av behandling vid avtalets slut	Specificera – tidsfrister för t.ex. radering att personuppgifter, loggar m.m.	jfr 28.3 g) GDPR	11

Vindelns Kommun

Avtalspunkt	Kommentar	Artikel i GDPR	Finns uppgiften med? Ja, delvis eller nej? Beskriv vad som saknas
Revision	Specificera hur revision ska genomföras, vad den ska visa och hur resultaten ska redovisas.	jfr 28.3 h) GDPR	5:5
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 personuppgifts- behandling i strid med instruktioner, detta avtal eller gällande dataskyddsregler ska PuB hålla PuA skadeslös.		10
Åtgärd om PuB anser att behandlingen är olaglig	Specificera vad PuB ska göra om de anser att behandlingen är olaglig samt vem som beslutar om att behandlingen ska upphöra	jfr 28.3 andra st GDPR	3:1
Avtalsperiod			11
Tvistelösningar	Hur ska tvister avgöras, i vilken domstol ska tvister avgöras		12