

Riktlinjer för en sammanhållen hantering av personuppgifter i Kils kommunkoncern

1 INLEDNING

Den europeiska dataskyddsförordningen, GDPR, med kompletterade dataskyddslag i Sverige, kräver att personuppgiftsbiträdesavtal (PUB-avtal) tecknas mellan personuppgiftsansvariga och personuppgiftsbiträden. I dessa avtal beskrivs och kravställs hanteringen av personuppgifter som ett biträde utför på uppdrag av den ansvarige.

Inom kommunal verksamhet är det nämnder och kommunala bolagsstyrelser som har rollen som personuppgiftsansvariga, och ibland även rollen som personuppgiftsbiträde mot andra personuppgiftsansvariga inom kommunkoncernen. Följden av det blir en komplex och svårförvaltd avtalskonstruktion.

Sveriges Kommuner och Regioner (SKR) har gjort bedömningen att PUB-avtal mellan kommunala nämnder kan ersättas med en så kallad ”rättsakt”.¹ Kils kommun bedömer att detta bör kunna omfatta även de kommunala bolagen.

De här föreliggande riktlinjerna utgör en sådan rättsakt som avser att ersätta PUB-avtal. Riktlinjerna följer i tillämpliga delar SKR:s mall för PUB-avtal, version 1.1.²

¹ Behövs biträdesavtal internt inom den kommunala förvaltningen?
<https://skl.se/download/18.49f0902a162d5414b69f036a/1524840432329/>

² SKL mall för personuppgiftsbiträdesavtal
https://skl.se/download/18.4e8f842167c692a03510550/1545293310296/pubavtal_1_1_181219_md5_521a94a04eb0385395eb705fe7c38d2e.docx

Kils kommun	Postadress	Besöksadress	Telefon	0554-191 00	Bankgiro	109-6510
	Box 88	Kommunhuset	Fax	0554-129 74	Plusgiro	12 21 10-0
	665 23 Kil	Östra Torggatan 2D	E-post	kommun@kil.se	Org.nr	212000-1751

2 DEFINITIONER

Behandling	En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddslagstiftning	Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den personuppgiftsbehandling som sker enligt denna Riktlinje, inklusive nationell sådan lagstiftning och EU-lagstiftning.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.
Instruktion	De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.
Logg	Logg är resultatet av Loggning.
Loggning	Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt denna Riktlinje och som kan knytas till en enskild fysisk person.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som överförts, lagrats eller på annat sätt Behandlats.
Registrerad	Fysisk person vars Personuppgifter Behandlas.
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).
Underbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.

3 BAKGRUND OCH SYFTE

3.1 Med dessa riktlinjer ("riktlinjen") reglerar den personuppgiftsansvarige personuppgiftsbitrådets behandling av personuppgifter åt den personuppgiftsansvarige. Riktlinjens syfte är att säkerställa den registrerades fri- och rättigheter vid behandlingen, i enlighet med vad stadgas i Allmänna dataskyddsförordningen EU 2016/679 ("dataskyddsförordningen"), art. 28.3.

3.2 Riktlinjens information, i form av bestämmelser och andra uppgifter som påverkar riktlinjens tillämpning, samt riktlinjens hänvisningar till sådan information, till exempel lagstiftning (inklusive förordningar och föreskrifter), avser vid var tid gällande sådan information.

4 BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den personuppgiftsansvarige utser personuppgiftsbiträdet för att utföra behandlingen för den personuppgiftsansvariges räkning enligt vad som stadgas i dessa riktlinjer.

4.2 Den personuppgiftsansvarige ska ge instruktioner till personuppgiftsbiträdet om hur det ska utföra behandlingen.

4.3. Personuppgiftsbiträdet får endast utföra behandlingen i enlighet med riktlinjen och vid var tid gällande instruktioner.

5 DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för behandlingen och för att utforma korrekta instruktioner så att personuppgiftsbiträdet och eventuella underbiträden kan fullgöra sitt eller sina uppdrag enligt dessa riktlinjer och huvudavtal i förekommande fall.

5.2 Den personuppgiftsansvarige ska utan onödigt dröjsmål informera personuppgiftsbiträdet om förändringar i behandlingen som påverkar personuppgiftsbitrådets skyldigheter enligt dataskyddslagstiftningen.

5.3 Den personuppgiftsansvarige ansvarar för att informera registrerade om behandlingen och för att tillvarata registrerades rättigheter enligt dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den personuppgiftsansvarige enligt dataskyddslagstiftningen.

6 PERSONUPPGIFTBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra behandlingen i enlighet med riktlinjen och instruktioner samt att följa dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda personuppgifterna mot alla slag av behandlingar som inte är förenliga med riktlinjen, instruktioner och dataskyddslagstiftningen.

6.3 Personuppgiftsbiträdet åtar sig säkerställa att samtliga fysiska personer som arbetar under dess ledning följer riktlinjen och instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

6.4 Personuppgiftsbiträdet ska på begäran från den personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt dataskyddsförordningen, art. 32-36, fullgörs och svara på begäran om utövande av den registrerades rättigheter i enlighet med dataskyddsförordningen, kap. III, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

6.5 Om personuppgiftsbiträdet finner att instruktionerna är otydliga, i strid med dataskyddslagstiftningen eller saknas och personuppgiftsbiträdet bedömer att nya eller kompletterande instruktioner är nödvändiga för att genomföra sina åtaganden ska personuppgiftsbiträdet utan dröjsmål informera den personuppgiftsansvarige, tillfälligt upphöra med behandlingen och invänta nya instruktioner.

6.6 Om den personuppgiftsansvarige förser personuppgiftsbiträdet med nya eller ändrade instruktioner ska personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den personuppgiftsansvarige huruvida genomförandet av de nya instruktionerna föranleder förändrade kostnader för personuppgiftsbiträdet.

7 SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla tekniska och organisatoriska säkerhetsåtgärder som krävs för att förhindra personuppgiftsincidenter, genom att säkerställa att behandlingen uppfyller kraven i dataskyddsförordningen och att den registrerades rättigheter skyddas.

7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den personuppgiftsansvarige, ska betraktas som nya instruktioner enligt riktlinjen.

7.4 Personuppgiftsbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till personuppgifterna för sådana fysiska personer som arbetar under personuppgiftsbitrådets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt logga åtkomst till personuppgifterna enligt riktlinjen i den utsträckning det krävs enligt instruktionen. Loggar får gallras först fem år efter loggningstillfället om inte annat

anges i instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med dataskyddslagstiftningen.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

8 SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, såvida inte annat avtalats.

8.2. Personuppgiftsbiträdet ska se till att samtliga fysiska personer som arbetar under dess ledning och deltar i behandlingen, är bundna av sekretessförbindelse avseende behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med eventuella underbiträden samt sekretessförbindelser mellan underbiträden och samtliga fysiska personer som arbetar under dess ledning, och som deltar i behandlingen.

8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den personuppgiftsansvarige eller agera för den personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende behandlingen.

8.4 Om den registrerade, tillsynsmyndighet eller tredje man begär information från personuppgiftsbiträdet som rör behandlingen, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om saken. Information om behandlingen får inte lämnas till den registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas. Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

9 GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål, på den personuppgiftsansvariges begäran, tillhandahålla den information om tekniska och organisatoriska säkerhetsåtgärder som den personuppgiftsansvarige behöver för

att kunna fastställa att personuppgiftsbiträdet uppfyller sina åtaganden enligt riktlinjen och dataskyddsförordningen, art. 28.3 h.

9.2 Personuppgiftsbiträdet åtar sig att minst en gång om året granska säkerheten avseende behandlingen genom en egenkontroll för att säkerställa att behandlingen följer riktlinjen. Resultatet av sådan egenkontroll ska på begäran delges den personuppgiftsansvarige.

9.3 Den personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till personuppgiftsbiträdet), följa upp att personuppgiftsbiträdet uppfyller riktlinjens, instruktionernas och dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den personuppgiftsansvarige, eller den som utför granskningen i den personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska personuppgiftsbitrådets efterlevnad av riktlinjen, instruktioner och dataskyddslagstiftningen. Den personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2-9.3, rätt att erbjuda andra tillvägagångssätt för granskning av behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska personuppgiftsbiträdet ge den personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

9.5 Personuppgiftsbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i riktlinjen.

9.6 Personuppgiftsbiträdet ska tillförsäkra den personuppgiftsansvarige rättigheter gentemot ett underbiträde, som motsvarar den personuppgiftsansvariges samtliga rättigheter gentemot personuppgiftsbiträdet enligt kap. 9 i riktlinjen.

10 HANTERING AV RÄTTELSE OCH RADERING M.M.

10.1 För det fall den personuppgiftsansvarige begärt rättelse eller radering på grund av personuppgiftsbitrådets felaktiga behandling ska personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom 30 dagar, från det att

personuppgiftsbiträdet mottagit erforderlig information från den personuppgiftsansvarige. När den personuppgiftsansvarige begärt radering får personuppgiftsbiträdet endast utföra behandling av den aktuella personuppgiften som ett led i processen för radering.

10.2 Om tekniska och organisatoriska åtgärder (till exempel uppgraderingar eller felsökningar) vidtas av personuppgiftsbiträdet i behandlingen, vilka kan väntas påverka behandlingen, ska personuppgiftsbiträdet informera den personuppgiftsansvarige skriftligt om detta i enlighet med vad stadgas om meddelanden i 19 kap. i riktlinjen. Informationen ska lämnas i god tid innan åtgärderna vidtas.

11 PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt dataskyddsförordningen, art. 32.1 c.

11.2 Personuppgiftsbiträdet åtar sig att med beaktande av behandlingens art, och den information som personuppgiftsbiträdet har att tillgå, bistå den personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en personuppgiftsincident beträffande behandlingen. Personuppgiftsbiträdet ska på den personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörig behandling och/eller åtkomst till personuppgifterna.

11.3 Vid personuppgiftsincidenter, som personuppgiftsbiträdet fått vetskap om, ska personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå tillhandahålla den personuppgiftsansvarige en skriftlig beskrivning av personuppgiftsincidenten.

Beskrivningen ska redogöra för:

- Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
- de sannolika konsekvenserna av personuppgiftsincidenten, och
- åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra personuppgiftsincidentens potentiella negativa effekter.

11.4 Om det inte är möjligt för personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkt 11.3 i riktlinjen, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

12 UNDERBITRÄDE

12.1 Personuppgiftsbiträdet ansvarar fullt ut för underbitrådets behandling gentemot den personuppgiftsansvarige.

12.2 Personuppgiftsbiträdet äger rätt att anlita ett nytt underbiträde. När personuppgiftsbiträdet avser att anlita ett nytt underbiträde ska personuppgiftsbiträdet säkerställa underbitrådets kapacitet och förmåga att uppfylla sina skyldigheter enligt dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den personuppgiftsansvarige om

- underbitrådets namn, organisationsnummer och säte (adress och land),
- vilken typ av uppgifter och kategorier av registrerade som behandlas, och
- var personuppgifterna ska behandlas.

12.3 Personuppgiftsbiträdet äger rätt att upphöra med att anlita underbiträdet. När personuppgiftsbiträdet upphör med att anlita underbiträdet ska personuppgiftsbiträdet skriftligen meddela den personuppgiftsansvarige om att det upphör med att anlita underbiträdet.

12.4 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt personuppgiftsbiträdesavtal med det nya underbiträdet och säkerställa att det nya underbiträdet åläggs samma skyldigheter som personuppgiftsbiträdet åläggs enligt denna riktlinje.

12.5 Personuppgiftsbiträdet ska på den personuppgiftsansvariges begäran översända en kopia av det personuppgiftsbiträdesavtal som personuppgiftsbiträdet tecknat med underbiträdet.

12.6 Den personuppgiftsansvarige äger inom 30 dagar rätt att invända mot personuppgiftsbitrådets anlitan av ett nytt underbiträde och att, med anledning av sådan invändning, säga upp denna riktlinje att upphöra i enlighet med vad stadgas i riktlinjen, punkt 17.4.

13 LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte riktlinjens parter kommer överens om något annat.

13.2 Personuppgiftsbiträdet äger endast rätt att överföra personuppgifter till tredje land för behandling (till exempel service, support, underhåll, utveckling, drift eller liknande hantering) om den personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat instruktioner för detta ändamål.

13.3 Överföring till tredje land för behandling enligt riktlinjen, punkt 13.2, får endast ske om den är förenlig med dataskyddslagstiftningen och uppfyller de krav på behandlingen som ställs i riktlinjen och instruktioner.

14 ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med behandling som, genom fastställd dom eller förlikning, ska utgå till den registrerade på grund av överträdelse av bestämmelse i riktlinjen, instruktioner och/eller tillämplig bestämmelse i dataskyddslagstiftningen ska art. 82 i dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter enligt dataskyddsförordningen, art. 83, eller lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 6 kap. 2 § ska bäras av den av de parter som påförts en sådan avgift.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad sägs i avtal mellan parterna gäller denna riktlinje, punkter 14.1 och 14.2, före andra regler om fördelning mellan parterna av krav sinsemellan såvitt avser behandlingen.

15 LAGVAL OCH TVISTELÖSNING

För denna riktlinje gäller svensk rätt. Eventuell tolkning eller tvist i anledning av riktlinjen, som parterna inte kan lösa på egen hand, ska avgöras av kommunfullmäktiges presidium.

16 RIKTLINJENS GILTIGHET

16.1 Riktlinjen gäller för alla nämnder och förvaltningar inom Kils kommun från och med den tidpunkt riktlinjen beslutats av kommunfullmäktige och tills vidare.

De kommunala bolagen ska följa koncerngemensamma direktiv beslutade i kommunfullmäktige vilket beskrivs i respektive bolags ägardirektiv. Riktlinjen omfattar således även de kommunala bolag där kommunen är majoritetsägare.

17 ÄNDRINGAR M.M.

17.1 Tillägg till, och ändringar i, riktlinjen ska vara skriftliga och beslutade av kommunfullmäktige.

17.2 Om någon som omfattas av riktlinjerna får kännedom om att motparten agerar i strid med riktlinjen, instruktioner och/eller dataskyddslagstiftningen, ska parten utan dröjsmål meddela motparten om agerandet.

18 ÅTGÄRDER VID RIKTLINJENS UPPHÖRANDE

18.1 Vid förändringar som innebär att personuppgiftsbiträdet inte längre utför behandlingen av personuppgifter ska den personuppgiftsansvarige utan onödigt dröjsmål begära att personuppgiftsbiträdet överlämnar samtliga personuppgifter till den personuppgiftsansvarige eller raderar dem, enligt dennes önskemål. Om personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga personuppgifter avses alla personuppgifter som har omfattats av behandlingen samt annan tillhörande information såsom loggar, instruktioner, systemlösningar, beskrivningar och andra handlingar som personuppgiftsbiträdet fått genom informationsutbyte enligt riktlinjen.

18.2 Överlämning och radering enligt riktlinjen, punkt 18.1, ska vara utförda senast 30 dagar räknat från den tidpunkt uppsägning gjorts enligt denna riktlinje, punkt 16.1

18.3 Behandling som utförs av personuppgiftsbiträdet efter den tidpunkt som stadgas i punkt 18.2 är att betrakta som en otillåten behandling.

18.4 Bestämmelser om sekretess/tystnadsplikt i 8 kap. riktlinjen ska fortsätta gälla även om riktlinjen i övrigt upphör av gälla.

19 MEDDELANDEN INOM RAMEN FÖR DENNA RIKTLINJE OCH INSTRUKTIONER

19.1 Meddelanden om riktlinjen och dess administration ska skickas till respektive parts kontaktperson för riktlinjen.

19.2 Meddelanden om parternas samarbete om dataskydd, gällande behandlingen, ska skickas till respektive parts kontaktperson för parternas samarbete om dataskydd.

19.3 Meddelanden inom ramen för riktlinjen och instruktioner ska skickas skriftligt. Ett meddelande ska anses ha kommit fram till mottagaren senast en arbetsdag efter att meddelandet har skickats.

20 KONTAKTPERSONER

20.1 Parterna ska utse var sin kontaktperson för riktlinjen.

20.2 Parterna ska utse var sin kontaktperson (dataskyddssamordnare) för parternas samarbete om dataskydd.

Kommunfullmäktige godkände dessa riktlinjer 2020-09-24, § 106.