

M0161 Mall för redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av Resebyråttjänster

Innehåll

1 Inledning.....	1
2 Kravkatalog	3
Följande krav kan i ett avrop kompletteras med	3
Följande villkor för fullgörande av kontraktet kan preciseras.....	3
3 Kvalificeringskrav.....	4
Krav på ramavtalsleverantörens informationssäkerhetsarbete	4
4 Tekniska krav	6
Informationssäkerhetskrav på upphandlingsföremålet	6
5 Tilldelningskriterier	6
Tilldelningskriterier avseende informationssäkerhet	6
6 Särskilda kontraktsvillkor.....	6
Villkor för informationssäkerhet vid fullgörande av ramavtalet.....	6

1 Inledning

Detta dokument redovisar krav och villkor avseende informationssäkerhet som använts i ramavtalsupphandling av Resebyråttjänster. Det innehåller även krav som kan ställas vid avrop. Dokumentet är avsett att ge en bild av hur frågor avseende informationssäkerhet hanterats i den aktuella ramavtalsupphandlingen.

Krav och villkor är hämtade från upphandlingsunderlag och ramavtal. För de fullständiga dokumenten hänvisas till information om respektive ramavtalsområde på avropa.se.



Kraven och villkoren är här indelade på följande sätt:

Kravkatalog

Kravkatalogen innehåller krav och villkor avseende informationssäkerhet som kan ligga till grund för kompletteringar och preciseringar vid avrop. Den avropsberättigade kan välja ut och formulera lämpliga krav.

Kvalificeringskrav

Kvalificeringskrav är obligatoriska krav på leverantören som ska vara uppfyllda redan när anbud lämnas in.

Tekniska krav

Tekniska krav avser obligatoriska krav på upphandlingsföremålet, produkten och eller tjänsten ställda i ramavtalsupphandlingen. Dessa krav kan vara uttryckta som ”ska-krav”.

Tilldelningskriterier

Tilldelningskriterier avser krav på egenskaper hos upphandlingsföremålet, produkten och eller tjänsten, som gett ett mervärde i ramavtalsupphandlingen, exempelvis poäng, påslag eller avdrag. Dessa krav kan vara uttryckta som ”bör-krav”.

Särskilda kontraktsvillkor

Särskilda kontraktsvillkor är krav och villkor som leverantör och upphandlingsföremål ska uppfylla vid ramavtalets fullgörande. Dessa villkor finns i ramavtalets Huvuddokument och i Allmänna villkor samt i Kravkatalog. Även andra benämningar förekommer.

2 Kravkatalog

Följande krav kan i ett avrop kompletteras med

Krav avseende informationssäkerhet på upphandlingsföremålet

Ur Bilaga Kravkatalog avsnitt Säkerhet:

9.2.3 Säkerhet

9.2.3.1 Säkerhetsskyddsavtal

Krav kan exempelvis ställas på säkerhetsskyddsavtal nivå 2 eller 3.

9.2.3.2 Säkerhet i Applikation till smartphone eller likvärdig lösning

Krav kan exempelvis ställas på att inloggning i app ska ske med två-faktor autentisering och att förbindelse mellan applikationen mellan applikation till smartphone eller alternativ lösning och tjänsten ska vara krypterad med TLS 1.2. Krav kan också ställas på att applikation till smartphone eller likvärdig lösning inte får använda sig av kamera, mikrofon och GPS.

Följande villkor för fullgörande av kontraktet kan preciseras

Informationen hämtad från Allmänna villkor avsnitt 7.16 Säkerhet och säkerhetsskyddsavtal

Ramavtalsleverantören ska följa de krav och villkor för säkerhet, gällande exempelvis informationssäkerhet, it-säkerhet, fysisk säkerhet och personalsäkerhet, som Avropsberättigad bestämmer samt se till att samtlig personal som direkt medverkar till att fullgöra Kontraktet följer dessa krav och villkor.

Om Avrop enligt Avropsberättigad omfattas av säkerhetsskydd enligt säkerhetsskyddslagen (2018:585), ska tillämpliga bestämmelser i nämnda lag följas. Ramavtalsleverantören och berörd Underleverantör ska på begäran ingå säkerhetsskyddsavtal med Avropsberättigad på den nivå och enligt de villkor som Avropsberättigad bestämmer. I sådana fall är Kontraktets giltighet villkorad av att ett gällande säkerhetsskyddsavtal föreligger mellan Avropsberättigad och Ramavtalsleverantören.



Ramavtalsleverantören har inte rätt till ersättning om Avropsberättigad säger upp Kontraktet till följd av att det saknas ett giltigt säkerhetsskyddsavtal. Säkerhetsskyddsavtalet ska inte omfatta affärsmässiga villkor såsom avgifter, viten, betalning och liknande.

7.17 Behandling av personuppgifter

Behandling av personuppgifter ska följa Europeiska unionens dataskyddsförordning (EU) 2016/679 med tillhörande genomförandeförfattningar (dataskyddsregleringen).

Ramavtalsleverantören ska vidta de nödvändiga tekniska och organisatoriska åtgärder som krävs för att skydda de personuppgifter som behandlas. Ramavtalsleverantör ska på begäran av Avropsberättigad ingå de avtal som krävs för att uppfylla dataskyddsregleringen.

3 Kvalificeringskrav

Krav på ramavtalsleverantörens informationssäkerhetsarbete

Information hämtad från Upphandlingsdokument avsnitt 4.2 Åberopande av andra företags kapacitet och avsnitt 4.6.5 Systematiskt informationssäkerhetsarbete

4.2 Åberopande av andra företags kapacitet

Anbudsgivaren har möjlighet att åberopa andra företags kapacitet för att uppfylla kvalificeringskrav som avser ekonomisk och finansiell ställning enligt avsnitt Ekonomisk och finansiell ställning eller teknisk och yrkesmässig kapacitet enligt avsnitt Teknisk och yrkesmässig kapacitet med undantag för avsnitt IATA. Dvs. anbudsgivaren får inte åberopa andra företags kapacitet för att uppfylla krav i avsnitten Kvalitetssäkringsarbete eller Systematiskt informationssäkerhetsarbete. Med andra företag avses exempelvis företag både inom och utom en koncern. Dessa benämns i upphandlingen som åberopat företag. Om ett åberopat företag inte uppfyller nedanstående krav för vilket det åberopas för, kan detta påverka anbudsgivarens anbud negativt.

I anbudsprocessen finns ett processteg i Mercell TendSign för att lägga till åberopade företag (benämns i Mercell TendSign som underleverantörer). I detta steg går det att söka fram företag i Mercell TendSign, eller registrera nya direkt i Mercell TendSign. Därefter ska anbudsgivaren välja att den tillagda underleverantören åberopas för kapacitet (dvs. för att uppfylla kraven i detta kapitel). För åberopat företag ska



anbudsgivaren sedan lämna egenförsäkran direkt i kapitel Uteslutning och kvalificering av anbudsgivare, för varje åberopat företag som lagts till.

Anbudsgivare ska som kompletterande dokument lämna in ett skriftligt åtagande från åberopat företag om att anbudsgivaren förfogar över åberopade resurser enligt avsnitt Kvalificeringskrav. Om det åberopade företaget åberopas för sin ekonomiska och finansiella ställning ska det åberopade företaget åta sig ett solidariskt ansvar för Ramavtalsleverantörens ekonomiska och finansiella åtaganden enligt Ramavtalet och Kontrakt.

Ett åberopat företag ska ha tillräcklig kapacitet och resurser för den del av tjänsten som företaget åberopas för. Ett åberopat företag kan förekomma i flera anbud så länge det åberopade företagets totala leveranskapacitet inte överskrids. Det åberopade företaget ska således inte erbjuda samma konsult till olika anbudsgivare.

Samarbetsformer En anbudsgivare (A) ska inte ingå som åberopat företag eller underleverantör till annan anbudsgivare (B) (inom samma anbudsområde). I de fall A trots detta ingår som åberopat företag till B, och B kan visa att den förfogar över A:s kapacitet, kommer A:s anbud i denna del inte att godkännas.

4.6.5 Systematiskt informationssäkerhetsarbete

Anbudsgivaren ska bedriva ett systematiskt informationssäkerhetsarbete som minst har en koppling till Upphandlingsföremålet.

Inom ramen för det systematiska informationssäkerhetsarbetet ska anbudsgivaren arbeta efter en upprättad informationssäkerhetspolicy som har en koppling till Upphandlingsföremålet och som minst säkerställer:

1. att det finns fastställda informationssäkerhetsmål,
2. att anbudsgivaren arbetar med uppföljning av fastställda informationssäkerhetsmål,
3. att anbudsgivaren arbetar med att identifiera risker utifrån fastställda informationssäkerhetsmål,
4. att anbudsgivaren arbetar med att hantera risker utifrån fastställda informationssäkerhetsmål, och
5. att anbudsgivaren har fördelat resurser samt tilldelat behörighet och befogenheter vad gäller informationssäkerhetsarbetet i dessa delar.

Kravet styrks genom att anbudsgivaren som kompletterande dokument lämnar en utförlig beskrivning av systematiskt informationssäkerhetsarbetet av vilken det framgår att punkterna 1-5 ovan är uppfyllda alternativt lämnar en kopia på giltigt certifikat enligt ISO 27001 eller annan certifiering som inkluderar de ovan nämnda rutinerna.



Handlingen ska vara översatt till svenska, engelska, danska eller norska om originalhandlingens är upprättad på ett annat språk.

4 Tekniska krav

Informationssäkerhetskrav på upphandlingsföremålet

Inga tekniska krav har ställts avseende informationssäkerhet

5 Tilldelningskriterier

Tilldelningskriterier avseende informationssäkerhet

Inga tilldelningskriterier avseende informationssäkerhet användes vid utvärderingen i ramavtalsupphandlingen.

6 Särskilda kontraktsvillkor

Villkor för informationssäkerhet vid fullgörande av ramavtalet

Information hämtad från Upphandlingsdokument avsnitt 6.12 Underleverantörer och 7.17.1 Konsekvensbedömning av dataöverföringar (Transfer Impact Assessment, TIA)

6.12 Underleverantör

Ramavtalsleverantören ska säkerställa att anlita Underleverantör uppfyller krav och villkor i Ramavtalet och Kontrakt avseende de delar av Upphandlingsföremålet som Underleverantör ska utföra, i alla led.



Ramavtalsleverantören ska på begäran tillhandahålla information om Underleverantör. Exempel på uppgifter är namn, vilka delar, i vilken utsträckning och under vilken tidsperiod Underleverantören medverkar till att fullgöra Kontrakt.

Ramavtalsleverantören ska ha rutiner och verka för att Underleverantörer åtar sig att de inte omfattas av någon av uteslutningsgrunderna i 13 kap. 1–3 §§ LOU samt att Underleverantörer i relevanta delar och vid fullgörande av Ramavtalet och Kontrakt, följer:

- Ramavtalsleverantörens kvalitetssäkringsarbete,
- Ramavtalsleverantörens krav på informationssäkerhet,
- kraven och villkoren i avsnitt Miljöhänsyn, och
- kraven och villkoren i avsnitt Antidiskriminering.

Ramavtalsleverantören ska om nödvändigt styrka att Underleverantör uppfyller relevanta krav och villkor. Ramavtalsleverantören ska också säkerställa att Underleverantör medverkar vid uppföljning enligt avsnitt Uppföljning.

Ramavtalsleverantören har inte rätt att till Underleverantör delegera rätten att ta emot Avropsförfrågan, lämna Avropssvar, teckna Kontrakt eller fakturera Avropsberättigad.

Ramavtalsleverantören (inklusive konsortiedeltagare) får inte vara Underleverantör till en annan Ramavtalsleverantör.

I punkterna nedan listas olika kategorier av Underleverantörer, vilka i Ramavtalet benämns särskilda Underleverantörer, eftersom de omfattas av särskilda villkor. Kategorierna omfattar alla led i leverantörskedjan. Ramavtalsleverantören får inte i Avropssvar använda särskild Underleverantör förrän bilaga Anmälan om särskild Underleverantör har skickats in till Kammarkollegiet. Ramavtalsleverantören kan lägga till, byta eller ta bort särskilda Underleverantörer genom att skicka in bilaga Anmälan om särskild Underleverantör för att fullgöra hela eller delar av det åtagande som framgår av Ramavtalet och Kontrakt. Särskilda Underleverantörer som redan är godkända i samband med upphandlingen behöver däremot inte anmälas.

- Företag vars kapacitet Ramavtalsleverantören åberopar för att uppfylla krav på ekonomisk och finansiell ställning eller teknisk och yrkesmässig kapacitet.
- Underleverantörer som kommer att fullgöra en väsentlig del av Ramavtalsleverantörens Kontrakt. Underleverantör anses utföra en väsentlig del av Kontrakten om delen utgör minst 10 procent av Ramavtalsleverantörens totala försäljning enligt Ramavtalet.
- Underleverantörer vars personal har eller kommer att ha direkt kontakt med Kammarkollegiet eller Avropsberättigad.



När det gäller en Underleverantör i första punkten, det vill säga ett åberopat företag, får inte Ramavtalsleverantören tilldelas Kontrakt förrän Kammarkollegiet skriftligen har godkänt det åberopade företaget. Kammarkollegiet kan ge Avropsberättigad rätten att godkänna det åberopade företaget. Till anmälan om att använda ett åberopat företag ska Ramavtalsleverantören bifoga ett skriftligt samarbetsavtal eller liknande med ett åtagande från företaget om att Ramavtalsleverantören kommer att förfoga över de nödvändiga resurserna samt vilka resurser företaget åberopas för. Om det åberopade företaget åberopas för sin ekonomiska och finansiella ställning ska det åberopade företaget åta sig ett solidariskt ansvar för Ramavtalsleverantörens ekonomiska och finansiella åtaganden enligt Ramavtalet och Kontrakt.

Om en Underleverantör bryter mot krav eller villkor som anges i Ramavtalet eller Kontrakt har Kammarkollegiet rätt att med omedelbar verkan bestämma att Underleverantören inte längre får anlitas för fullgörande av Ramavtalet eller Kontrakt.

Ramavtalsleverantören ansvarar för sina Underleverantörer såsom för egen del. Om Ramavtalsleverantören inte uppfyller ovanstående krav och villkor kan det resultera i vite och andra påföljder enligt avsnitt Avtalsbrott och påföljder.

7.17.1 Konsekvensbedömning av dataöverföringar (Transfer Impact Assessment, TIA)

Ramavtalsleverantören ska ha fastställda rutiner för att genomföra en konsekvensbedömning av dataöverföringar (Transfer Impact Assessment), i enlighet med Europeiska dataskyddsstyrelsens rekommendationer 01/2020. Ramavtalsleverantören ansvarar också för att Underleverantörer som anlitas för att fullgöra Kontrakt har sådana rutiner. I Kontrakt som innefattar överföring av personuppgifter till tredje land ska Ramavtalsleverantören eller Underleverantör innan Kontraktets fullgörande ha genomfört en TIA. Ramavtalsleverantören ska på Avropsberättigads begäran överlämna analysen.