Redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av Programvaror och tjänster - Systemutveckling

Innehåll

Box 2218, 103 15 Stockholm
Birger Jarlsgatan 16, Stockholm
www.kammarkollegiet.se
registratur@kammarkollegiet.se
Telefon 08-700 08 00
Telefax 08-700 09 98
Organisationsnummer 202100-0829

1 Inledning

Detta dokument redovisar krav och villkor avseende informationssäkerhet som använts i ramavtalsupphandling av Programvaror och tjänster - Systemutveckling. 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 upphandlingsförmålet, 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 upphandlingsförmål 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

Exempel på krav enligt bilaga Kravkatalog:

Certifiering
Vid Avrop kan krav komma att ställas utifrån Programvaras certifiering för exempelvis viss hårdvara, operativsystem, andra Programvaror eller säkerhetsklassning.

Dataskyddsförordningen
Vid avrop kan krav komma att ställas på Ramavtalsleverantören gällande förhållanden enligt dataskyddsförordningen, exempelvis krav gällande överföring av personuppgifter till tredje land. Observera att nedan beskrivning av respektive parameter inte är uttömmande utan endast exemplifierar hur dessa kan användas vid avrop. Det kan röra sig om krav gällande redogörelse om:

• till vilket land eller vilka länder som aktuella personuppgifter kommer att överföras eller från vilket land eller vilka länder som mottagaren av personuppgifterna skulle ha tillgång till aktuella personuppgifter.

• vem eller vilka som är mottagare av aktuella personuppgifter.

• vilka typer av tjänster som mottagaren tillhandahåller och för vilka mottagaren skulle behandla överförda personuppgifter.

• för vilket eller vilka ändamål som överföringen kommer att genomföras och den efterföljande behandlingen, ex. om personuppgifterna kommer att användas för test och utveckling eller för framställande av statistik.

• på vilket sätt personuppgifterna kommer att överföras till mottagaren och på vilket sätt mottagaren därefter kommer att behandla desamma.

• med stöd av vilket överföringsverktyg, alternativt med stöd av vilken undantagsbestämmelse, som överföringen skulle ske.

• vilka typer och kategorier av personuppgifter som omfattas av överföringen.

• i vilken omfattning som personuppgifter skulle överföras till mottagaren (volymen av personuppgifter).

• hur ofta som berörda personuppgifter kommer att överföras till mottagaren (t.ex. löpande, månatligen eller en gång).

• integritetskänsliga eller särskilda kategorier av personuppgifter omfattas av överföringen.

• vilka kategorier av registrerade individer som berörs av överföringen.

• mottagaren är en molntjänstleverantör eller en leverantör av kommunikationstjänster.

• i vilken eller vilka sektorer som mottagaren är verksam.

• i vilket format som personuppgifter kommer att överföras till mottagaren och eventuellt lagras hos mottagaren.

• på vilket sätt mottagarens tillgång till berörda personuppgifter kan kontrolleras (t.ex. genom åtkomstkontroller och behörighetsstyrning).

• för de fall ramavtalsleverantören omfattas av lagstiftning i mottagarlandet och den aktuella lagstiftningen är tillämplig på överföringen, om det finns en reell risk för att överföringen innebär att myndigheterna i mottagarlandet med framgång skulle kunna få åtkomst till uppgifterna.

• att ramavtalsleverantören kommer att agera lojalt i enlighet med kontrakt trots att denne omfattas av lagstiftning i mottagarlandet som påverkar skyddet för överförda personuppgifter.

• och i vilket utsträckning berörda personuppgifter överförs och lagras krypterat, med vilken krypteringsteknik, hur krypteringsnyckeln lagras och i vilken miljö dekryptering av berörda personuppgifter sker.

• och i vilken utsträckning berörda personuppgifter pseudonymiseras innan överföring till mottagaren och vid eventuell lagring hos mottagaren.

• de begäranden som mottagaren i tredje land tagit emot från offentliga myndigheter i mottagarlandet om tillgång till personuppgifter som mottagaren behandlar. Det kan exempelvis vara information om antalet begäranden, typ av uppgifter som begärts, uppgift om den eller de begärande myndigheterna, om begärandena har bestridits och resultatet av bestridandena.

Informationssäkerhet
Vid Avrop kan krav komma att ställas på informationssäkerhet, t.ex. behörighet, loggning, certifiering samt möjlighet att sätta rättigheter.

Personuppgiftsbehandling och Personuppgiftsbiträdesavtal.
Vid Avrop kan krav komma att ställas på att Ramavtalsleverantör och Underleverantör ingår Personuppgiftsbiträdesavtal med Kund.

Säkerhet
Med Säkerhet avses både aktiviteter rörande it-säkerhet, informationssäkerhet och säkerhetsskydd. Exempel på Säkerhet är säkerhetsanalys av Programvara och molntjänst, informationsklassificering, risk- och sårbarhetsanalys, utforma regelverk och processer runt säkerhet i Programvara och molntjänst, leda säkerhetsarbetet vid skapande av it-system, informationssäkerhetsrelaterad kravhantering, hantera loggar och loggning samt hantering av behörigheter.

Avsnitt Säkerhet och Säkerhetsskyddsavtal
Vid Avrop kan krav komma att ställas på säkerhet och på att Ramavtalsleverantör och Underleverantör ingår Säkerhetsskyddsavtal med Kund. Vid Avrop av Konsulttjänst kan krav komma att ställas på registerkontroll och särskild personutredning av Konsult.

Krav kan också komma att ställas i syfte att uppfylla krav i de för statliga myndigheter gällande föreskrifter MSBFS 2020:6, MSBFS 2020:7, MSBFS 2020:8 och tillkommande publikationer från MSB. Dessa krav kan ställas av alla avropsberättigade.

Följande villkor för fullgörande av kontraktet kan preciseras

Se ovan.

3 Kvalificeringskrav

Krav på ramavtalsleverantörens informationssäkerhetsarbete

Inga kvalificeringskrav avseende informationssäkerhetsarbete har ställts.

4 Tekniska krav

Informationssäkerhetskrav på upphandlingsföremålet

4.6 Informationssäkerhet i molntjänst

4.5.1 Autentisering och auktorisering.
Molntjänst som erbjuds av anbudsgivaren ska skyddas mot obehörig åtkomst genom autentisering och auktorisering.

4.5.2 Skydd mot skadlig kod.
Molntjänst som erbjuds av anbudsgivaren ska tillhandahålla skydd mot skadlig kod.

4.5.3 Krypterad lagringsmedia.
Fasta och löstagbara lagringsmedia som lagrar kunds information i en privat molntjänst ska kunna vara krypterade.

4.5.4 Krypterad datorkommunikation.
Kunds information som inom ramen för en molntjänst överförs via datorkommunikation ska skyddas med kryptering. Kravet gäller både mellan olika datacenter och mellan datacenter och kund.

4.5.5 Säkerhetskopiering.
Molntjänst som lagrar kunds information och som erbjuds av anbudsgivaren ska ha funktioner för att regelbundet överföra kunds information till säkerhetskopior. Säkerhetskopiorna ska förvaras avskilt och väl skyddade så att kunds information kan återskapas efter ett fel. Det ska finnas en rutin för test av återläsning.

4.5.6 Loggning.
Förändringar utförda av administratör av molntjänst som erbjuds av anbudsgivaren ska loggas.

5 Tilldelningskriterier

Tilldelningskriterier avseende informationssäkerhet

4.4.3 Informationssäkerhetskonsult som innehar giltig certifiering CISSP, CISM eller likvärdigt samt har arbetat med informationssäkerhet i uppdraget kan erhålla ytterligare 0,5 poäng.

6 Särskilda kontraktsvillkor

Villkor för informationssäkerhet vid fullgörande av ramavtalet

Kravkatalogen avsnitt Kontraktsvillkor Om ett Säkerhetsskyddsavtal och/eller Personuppgiftsbiträdesavtal tecknats och lagts som bilaga till Kontrakt och om något stadgande eller villkor i kontraktshandlingarna utgör hinder mot eller försvårar tillämpning av någon klausul i Säkerhetsskyddsavtalet och/eller Personuppgiftsbiträdesavtalet, gäller vad som avtalats i Säkerhetsskyddsavtalet och/eller Personuppgiftsbiträdesavtalet före Kontrakt.

Allmänna villkor, avsnitt 7.21 Säkerhet och säkerhetsskyddsavtal
Ramavtalsleverantör ska följa de föreskrifter och riktlinjer för säkerhet och informationssäkerhet som anges i Ramavtalet och Kontraktet, eller som Kund redovisar från tid till annan samt se till att berörd personal iakttar dessa föreskrifter. Process för och konsekvenser av ändringar i föreskrifter eller riktlinjer under Kontraktstid ska följa vad som framgår avsnitt Ändring av Kontrakt.

Om Avrop enligt Kund omfattas av säkerhetsskydd enligt säkerhetsskyddslagen, ska tillämpliga bestämmelser i nämnda lag beaktas. Om Kund begär det ska Ramavtalsleverantör och berörd Underleverantör ingå Säkerhetsskyddsavtal med Kund på den nivå som Kund begär och i förekommande fall på de villkor som Kund anger. I sådana fall är Kontrakts giltighet villkorat av att ett gällande Säkerhetsskyddsavtal föreligger mellan Kund och Ramavtalsleverantör. Ramavtalsleverantör har inte rätt till ersättning om Kund säger upp Kontrakt till följd av att gällande Säkerhetsskyddsavtal saknas. Säkerhetsskyddsavtal ska inte omfatta affärsmässiga villkor som avgifter, viten, betalning, etcetera. Ramavtalsleverantör ska vara väl införstådd med, samt följa Kunds säkerhetsangivelser vid tillträde till Kunds lokaler. Ramavtalsleverantör och dess Underleverantör är skyldig att följa samtliga bestämmelser i tecknat Säkerhetsskyddsavtal och bland annat tillse att Konsult medverkar vid avtalad säkerhetsprövning. För det fall Konsult inte medges utföra arbete för Kund efter sådan prövning, ska Ramavtalsleverantör utan dröjsmål tillse att annan lämplig Konsult ställs till Kunds förfogande.