M0161 Mall för redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av Programvaror och tjänster - Programvarulösningar

Innehåll

1 Inledning 2
2 Kravkatalog 4
Följande krav kan i ett avrop kompletteras med 4
3 Kvalificeringskrav 6
4 Begränsningskriterier 6
5 Tekniska krav 7
Informationssäkerhetskrav på upphandlingsföremålet 7
6 Tilldelningskriterier 8
7 Särskilda kontraktsvillkor 8
Villkor för informationssäkerhet vid fullgörande av ramavtalet 8

1 Inledning

Detta dokument redovisar krav och villkor avseende informationssäkerhet som använts i ramavtalsupphandling av Programvaror och tjänster – Programvarulösningar. 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.

Begränsningskriterier

Begränsningskriterier avser krav på leverantören som använts för att begränsa antalet leverantörer som bjuds in att lämna anbud. Dessa kan vara uttryckta som ”bör-krav”.

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

Ur Bilaga Kravkatalog:

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.

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 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.

3 Kvalificeringskrav

Inga kvalificeringskrav har ställts avseende informationssäkerhet.

4 Begränsningskriterier

Ur Anbudsinbjudan, kapitel 4.2 begränsningskriterier:

4.2.2 Ledningssystem för informationssäkerhet

Sökanden erhåller 10 poäng om sökanden har ett dokumenterat ledningssystem för informationssäkerhet för den egna verksamheten, med certifikat/diplom utfärdat av en oberoende tredje part.

Sökanden anger om ett dokumenterat ledningssystem för informationssäkerhet för den egna verksamheten finns, med certifikat/diplom utfärdat av en oberoende tredje part.

För att styrka ovanstående ska sökanden som kompletterande dokument inkomma med antingen

1. gällande certifikat för ISO 27001, eller
2. ett likvärdigt ledningssystem för informationssäkerhet som är certifierat av ackrediterat organ, i något land inom EES, och som minst omfattar:

    a. Policy för informationssäkerhet
    b. Upprättande och uppföljning av informationssäkerhetsmål för verksamheten
    c. Identifiering och hantering av risker
    d. Fastställa vilka resurser som behövs samt tilldela ansvar och befogenheter vad gäller informationssäkerheten

Ackrediteringsorganet ska vara medlem i eller ansluten till någon av de internationella organisationerna för ackrediteringsorgan, exempelvis:

- EA (European co-operation for Accreditation),
- IAF (International Accreditation Forum), eller
- ILAC (International Laboratory Accreditation Cooperation).

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

Notera att detta begränsningskriterium måste uppfyllas av sökanden självt för att poäng ska erhållas, dvs detta begränsningskriterium kan ej uppfyllas genom att åberopa annat företag.

5 Tekniska krav

Informationssäkerhetskrav på upphandlingsföremålet

Ur Anbudsinbjudan, kapitel Kravspecifikation:

4.6.1 Autentisering och auktorisering

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

4.6.2 Skydd mot skadlig kod

Molntjänst som erbjuds av anbudsgivaren ska vara skyddad mot skadlig kod.

4.6.3 Krypterad lagringsmedia

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

4.6.4 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.

4.6.5 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 dokumenterad rutin för test av återläsning.

4.6.6 Loggning

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

6 Tilldelningskriterier

Inga tilldelningskriterier avseende informationssäkerhet användes vid utvärderingen i ramavtalsupphandlingen.

7 Särskilda kontraktsvillkor

Villkor för informationssäkerhet vid fullgörande av ramavtalet

Ur Ramavtalets huvuddokument:

5.10.9 Ledningssystem för informationssäkerhet
Ramavtalsleverantören ska ha ett strukturerat och dokumenterat ledningssystem för informationssäkerhet för den egna verksamheten. Informationssäkerhetsarbetet ska vara aktivt under hela tiden Ramavtalet och Kontrakt är i kraft.

Ramavtalsleverantören ska på begäran från Kammarkollegiet eller Kund redovisa sitt ledningssystem för informationssäkerhet minst innehållande punkterna 1 - 5 nedan.

Som alternativ till redovisning av ledningssystem för informationssäkerhet i sig godtas att Ramavtalsleverantör redovisar gällande certifikat avseende ett ledningssystem för informationssäkerhet som minst motsvarar punkterna 1 - 5 nedan, samt kan redovisa kraven för certifiering till Kammarkollegiet. Certifikat som

redovisas ska vara utställt av ett ackrediterat certifieringsorgan som är medlem eller ansluten till någon av de internationella organisationerna för ackrediteringsorgan, exempelvis:

- EA (European co-operation for Accreditation),
- IAF (International Accreditation Forum), eller
- ILAC (International Laboratory Accreditation Cooperation).

1. Process för bedömning av informationssäkerhetsrisker

Fastställande och tillämpning av en process för bedömning av informationssäkerhetsrisker som upprättar och underhåller kriterier för riskacceptans och kriterier för bedömningar av informationssäkerhetsrisker. Processen ska säkerställa att upprepade bedömningar av informationssäkerhetsrisker genererar konsistenta, korrekta och jämförbara resultat. Processen ska omfatta att informationssäkerhetsriskerna identifieras genom tillämpning av processen för bedömning av informationssäkerhetsrisker för att identifiera risker förknippade med förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystem för informationssäkerhet. Processen ska omfatta att informationssäkerhetsriskerna analyseras genom att bedöma de potentiella konsekvenser som skulle uppstå om riskerna som identifierats realiseras. Vidare ska den realistiska sannolikheten för förekomsten av de risker som identifierats bedömas och risknivåer fastställas.

Informationssäkerhetsriskerna ska utvärderas och resultaten av riskanalyser jämföras med de fastställda riskkriterierna. De analyserade riskerna ska prioriteras för riskbehandling. Bedömningar av informationssäkerhetsrisker ska genomföras med planerade intervall eller när betydande förändringar föreslås eller uppstår, med hänsyn till de kriterier som fastställs.

2. Process för behandling av informationssäkerhetsrisker

Fastställande och tillämpning av en process för behandling av informationssäkerhetsrisker för att välja ut lämpliga alternativ för behandling av informationssäkerhetsrisker, med hänsyn tagen till resultaten av riskbedömningen samt fastställande av alla säkerhetsåtgärder som är nödvändiga för att införa valda alternativ för behandling av informationssäkerhetsrisker. Processen ska omfatta verifikation av att inga nödvändiga säkerhetsåtgärder har utelämnats. Processen ska leda till skapandet av ett uttalande om tillämplighet som innehåller de nödvändiga säkerhetsåtgärderna och motivering för inkludering samt om de är införda eller inte. Processen ska omfatta formulerandet av en plan för behandling av informationssäkerhetsrisker.

3. Process för upprättande och dokumentation av informationssäkerhetsmål

Fastställande och tillämpning av en process för upprättande och dokumentation av informationssäkerhetsmål för relevanta funktioner och nivåer. Informationssäkerhetsmålen ska vara mätbara (om det är praktiskt möjligt), beakta tillämpliga informationssäkerhetskrav och resultat från riskbedömning och riskbehandling, kommuniceras samt uppdateras efter behov.

4. Process för lämpligheten, tillräckligheten och verkan av ledningssystem

Fastställande och tillämpning av en process för att lämpligheten, tillräckligheten och verkan av ledningssystem för informationssäkerhet ständigt ska förbättras. Processen ska innefatta fastställande av vilka resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra ledningssystem för informationssäkerhet samt säkerställande av att resurserna tillhandahålls.

5. Genomförande av interna revisioner

Genomförande av interna revisioner med planerade intervall för att få information om huruvida ledningssystem för informationssäkerhet överensstämmer med kraven på ledningssystem för informationssäkerhet samt att ledningssystem för informationssäkerhet har införts och underhållits på ett ändamålsenligt sätt.

5.10.9.1 Kontinuitetsplan och skydd mot obehöriga

Ramavtalsleverantören ska ha en kontinuitetsplan för sin verksamhet och sina it-system. Kontinuitetsplanen ska testas regelbundet.

Ramavtalsleverantören ska skydda Kunds information som hanteras och förvaras i Ramavtalsleverantörens lokaler från obehöriga samt ha rutiner för hur denna information skyddas från obehöriga.