

Redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av rekryteringstjänster

Innehåll

1 Inledning.....	1
2 Kravkatalog	3
Krav, villkor och tilldelningskriterier avseende informationssäkerhet	3
3 Kvalificeringskrav.....	4
4 Tekniska krav	4
5 Tilldelningskriterier	5
6 Särskilda kontraktsvillkor.....	5
Villkor för informationssäkerhet vid fullgörande av ramavtalet.....	5

1 Inledning

Detta dokument redovisar krav och villkor avseende informationssäkerhet som använts i ramavtalsupphandling av rekryteringstjänster. 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 genom förnyad konkurrensutsättning. 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 i ramavtalsupphandlingen.

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

Krav, villkor och tilldelningskriterier avseende informationssäkerhet

Informationen hämtad från Avropsrutin avsnitt 9.5.5 Kravkatalog.

Utöver de krav som ställts i upphandlingen, kan Avropsberättigad använda nedanstående parametrar (se punkt 1-15) vid Avrop genom förnyad konkurrensutsättning. Parametrarna kan antingen ställas som obligatoriska krav, villkor i Kontrakt eller användas som tilldelningskriterier vid utvärdering av Avropssvar. Det är upp till Avropsberättigad att definiera hur respektive parameter ska användas. Om parametrarna används som tilldelningskriterier ska Avropsberättigad i Avropsförfrågan ange och specificera den inbördes vikten mellan tilldelningskriterierna och redogöra för vilken utvärderingsmodell som kommer att användas.

Observera att nedan beskrivning av respektive parameter inte är uttömmande utan endast exemplifierar hur dessa kan användas vid Avrop.

Följande parametrar kan användas vid Avrop genom förnyad konkurrensutsättning:

Punkt 10. Informationssäkerhet

- *Skydd av information mot obehörig åtkomst genom autentisering och auktorisering*
- *Brandväggar finns för de system som nyttjas inom ramen för utförandet av tjänsterna*
- *Loggar bevaras och granskas regelbundet*
- *Skydd av loggningsverktyg och logginformation mot manipulation och obehörig åtkomst*
- *Kryptering av fasta och löstagbara lagringsmedia som lagrar kunds information*
- *Regelbunden säkerhetskopiering av information som är tillhandahållen eller av stor vikt för kunder*

Punkt 11. Säkerhetsskydd

- *Tecknande av säkerhetsskyddsavtal*

Punkt 12. Personuppgiftsbehandling/GDPR

- *Tecknande av personuppgiftsbiträdesavtal och /eller datadelningsavtal*
- *Redogörelse gällande åtkomst av uppgifter hos Ramavtalsleverantören eller av denne anlita underleverantör (exempelvis leverantör som tillhandahåller*



rekryteringsverktyg) och hur denna åtkomst kan kontrolleras genom åtkomstkontroller och behörighetsstyrning

- Att Ramavtalsleverantören kommer att agera lojalt, i enlighet med Kontrakt, trots att denne omfattas av lagstiftning i mottagarlandet som påverkar skyddet för överförda personuppgifter
- Redogörelse gällande de begäranden som mottagaren (Ramavtalsleverantören eller av denne anlita underleverantör) 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
- Tillägg av överföringsmekanism och/eller angivande av kompletterande åtgärder för överföring av personuppgifter till ett tredje land med adekvansbeslut från EU-kommissionen, för det fall adekvansbeslutet skulle upphöra att gälla

Punkt 13. **Rekryteringsverktyg**

- Anpassat för efterlevnad av relevanta regulatoriska krav
- Anpassat för webbläsare som är vanligt förekommande på marknaden, såsom exempelvis Microsoft Edge eller Chrome
- Funktion som möjliggör kandidats inloggning med bank-id eller motsvarande för att ta del av tester och/eller information
- Funktion som möjliggör tvåfaktorsinloggning
- Funktion för återställande av förlorad information inom viss, av Avropsberättigad, angiven tid efter inkommen anmälan
- Funktion för dataexport i format som garanterar informationssäkerhet och som möjliggör återanvändning av informationen
- Driftas hos Ramavtalsleverantören inom Sverige eller EU
- On-premises lösning
- Garanti att lagring av personuppgifter endast kommer att ske inom vissa geografiska områden (exempelvis enbart inom EU/EES samt inom tredje land med adekvat skyddsnivå)
- Funktion för generande av automatiska påminnelser om radering/gallring av uppgifter i enlighet med Avropsberättigads gallringsföreskrifter
- Radering/gallring av information på sätt som gör att den inte kan återskapas

3 Kvalificeringskrav

Inga kvalificeringskrav har ställts avseende informationssäkerhet.

4 Tekniska krav

Inga tekniska krav har ställts avseende informationssäkerhet.



5 Tilldelningskriterier

Inga tilldelningskriterier avseende informationssäkerhet användes vid utvärderingen i ramavtalsupphandlingen.

6 Särskilda kontraktsvillkor

Villkor för informationssäkerhet vid fullgörande av ramavtalet

Informationen hämtad från Ramavtalets Huvuddokument avsnitt 11.9.9 Systematiskt informationssäkerhetsarbete.

Ramavtalsleverantören ska senast vid Ramavtalets ikraftträdande bedriva ett systematiskt informationssäkerhetsarbete som minst omfattar de system och den personal som nyttjas vid tillhandahållande av Upphandlingsföremål.

Inom ramen för det systematiska informationssäkerhetsarbetet ska Ramavtalsleverantören arbeta efter en upprättad och av ledningen beslutad informationssäkerhetspolicy som minst säkerställer följande.

- *Att det finns fastställda och mätbara informationssäkerhetsmål.*
- *Att det finns rutiner för att identifiera och hantera risker utifrån fastställda informationssäkerhetsmål.*
- *Att det finns rutiner för hantering och rapportering vid säkerhetsincidenter.*
- *Att det finns en tydlig ansvarsfördelning inom organisationen gällande informationssäkerhetsarbetet.*
- *Att anställda informeras regelbundet om hur information får hanteras.*
- *Att anställda har teknisk tillgång till kundens data enbart i de fall det är nödvändigt för att kunna fullgöra uppdrag enligt Kontrakt.*

Ramavtalsleverantören ska genomföra regelbundna revisioner av informationssäkerhetsarbetet och på begäran av Kammarkollegiet kunna visa upp relevant dokumentation som styrker efterlevnaden av ovan ställda krav.

Om Ramavtalsleverantören inte uppfyller ovanstående krav och villkor kan det resultera i vite och andra påföljder enligt avsnitt Avtalsbrott och påföljder.

Informationen hämtad från Allmänna villkor avsnitt 12.15 Säkerhet och säkerhetsskyddsavtal.

Om Avrop skett genom en förnyad konkurrensutsättning ska Ramavtalsleverantören 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.

Ramavtalsleverantören har rätt till ersättning för direkta, skäligen och verifierbara kostnader som uppstår till följd av genomförande av säkerhetsprövning av rekryteringskonsulten.

Informationen hämtad från Allmänna villkor avsnitt 12.16.1 Generella krav gällande behandling av personuppgifter.

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

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

Informationen hämtad från Allmänna villkor avsnitt 12.16.2 Överföring av personuppgifter till tredje land.

Ramavtalsleverantören ska ha fastställda rutiner för att genomföra en Transfer Impact Assessment (TIA), metodisk överföringsanalys, 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 anlita Underleverantör innan Kontraktets fullgörande ha genomfört en TIA/metodisk överföringsanalys. Ramavtalsleverantören ska på begäran av Avropsberättigad överlämna sådan genomförd analys.

Informationen hämtad från Allmänna villkor avsnitt 12.16.3 Behandling av personuppgifter i rekryteringsverktyg.

För det fall tjänsten innefattar personuppgiftsbehandling i ett av Ramavtalsleverantören tillhandahållet rekryteringsverktyg ska



Ramavtalsleverantören eller anlitad Underleverantör, i förhållande till Avropsberättigad, på begäran redogöra för vilka krav som ställts och åtgärder som vidtagits för att verktyget ska vara förenligt med dataskyddsregleringen. Behandling av känsliga personuppgifter, till exempel gällande en arbetssökandes hälsotillstånd, får inte ske i rekryteringsverktyget såvida inte annat särskilt angetts i Avropet eller överenskommit inför den specifika behandlingen. Personuppgifter i rekryteringsverktyg ska raderas eller avidentifieras så snart uppgifterna inte längre är nödvändiga för ansökningsförfarandet, efterföljande rättsliga åtgärder eller arkivändamål.

Informationen hämtad från Allmänna villkor avsnitt 12.16.4 Behandling av personuppgifter i samband med bakgrundskontroller.

Ramavtalsleverantören ska själv eller genom anlitad Underleverantör kunna genomföra bakgrundskontroller av kandidat. Det åligger Ramavtalsleverantören att tillförsäkra sig om att de personuppgifter som behandlas i samband med bakgrundskontroller följer dataskyddsförordningen och att eventuella tillstånd för behandling enligt artikel 10 i förordningen finns senast vid tidpunkten för tecknandet av Kontrakt som innefattar bakgrundskontroller. För det fall det inte framgår av Avropsförfrågan ska Ramavtalsleverantören inför leverans av bakgrundskontroll efterfråga på vilket sätt och i vilken omfattning Avropsberättigad önskar ta del av resultatet från genomförd bakgrundskontroll.