LÄNSRÄTTEN I STOCKHOLMS LÄN

DOM
2008-11-14
Meddelad i
Stockholm

Mål nr
20630-08
Rotel 202

SÖKANDE
Stepstone Solutions AB, 556512-7650

Ombud: David Sommestad
Östra Storgatan 3
611 34 Nyköping

MOTPART
Försäkringskassan
Processjuridiska enheten/Sundsvall
851 93 Sundsvall

SAKEN
Överprövning enligt lagen (2007:1091) om offentlig upphandling, LOU

DOMSLUT

Länsrätten bifaller ansökan och förordnar att upphandlingen skall göras om.

Postadress
115 76 Stockholm

Besöksadress
Tegeluddsvägen 1

Telefon
08-561 680 00

Telefax
08-561 680 01

E-post: lansrattenistockholm@dom.se

Expeditionstid
måndag – fredag
09:00-15:00

BAKGRUND OCH YRKANDEN M.M.

Försäkringskassan har inbjudit leverantörer att lämna anbud avseende IT-stöd av rekrytering baserat på ASP-tjänst (diarienr 17536-2008). Anbud skulle vara Försäkringskassan tillhanda senast den 15 oktober 2008.

Stepstone Solutions AB (Stepstone) har begärt överprövning av upphandlingen och yrkar i första hand att länsrätten beslutar att upphandlingen rättas på så vis att skall-kravet i svarsbilaga B, p. 2.3.6 *"personuppgifters lagring på server"* stryks i sin helhet. I andra hand yrkar Stepstone att upphandlingen skall göras om.

Försäkringskassan bestrider bifall till Stepstones yrkanden.

GRUNDER

Stepstone anför till stöd för sin talan i huvudsak följande. Stepstone uppfyller samtliga skall-krav i upphandlingens förfrågningsunderlag utom ett:
2.3.6 *Personuppgifters lagring på server*
Anbudsgivaren skall tillgodose att lagring och behandling av personuppgifter ska ske i Sverige, dvs. den server som används ska finnas och hanteras inom Sveriges gränser.
Stepstone har ifrågasatt detta krav och försökt förmå upphandlaren att justera detta krav så att server som skall användas till personuppgiftsbehandling kan placeras i vilket EU-land som helst, så länge anbudsgivare ingår säkerhetsskyddsavtal med Försäkringskassan och i övrigt uppfyller krav på sekretess och säkerhet. Försäkringskassan svarade att kravet inte kommer att ändras.

Att tillse att hemlig information förblir hemlig ställer givetvis stora krav på leverantören av en ASP-tjänst. Attacker mot servrar som innehåller känslig

information måste kunna mötas innan någon skada sker. Stepstone är väl medvetna om vilka krav som ställs på en ASP-leverantör. Kunder från ett flertal av Europas största företag använder Stepstones IT-stöd för rekryteringstjänster, bland de svenska kan nämnas Telia, SAS, Åklagarmyndigheten, FOI, Tullverket, Ekobrottsmyndigheten m.fl. Att erbjuda marknadsledande säkerhet för den information som kunderna lägger in i systemet är en självklarhet. De stora hoten mot informationssäkerheten ligger i serverintrång (hackning). Att någon skulle stjäla en server och därefter extrahera känslig information är mindre troligt. Serverns fysiska placering har därför en väldigt liten betydelse för säkerheten och skyddet för den information som den bär. En server som fysiskt är placerad inom Sveriges gränser blir inte per automatik mer säker än en server som är placerad i ett annat EU-land. Stepstones servrar är placerade i Belgien och i England. Om det är möjligt för ovan nämnda myndigheter att använda Stepstones rekryteringsverktyg, torde säkerhetsskyddet vara tillräckligt även för Försäkringskassan.

Försäkringskassan ställer som krav i aktuell upphandling att anbudsgivare som kontrakteras som leverantör skall ingå säkerhetsskyddsavtal med Försäkringskassan. Stepstone utgår från att säkerhetsskyddsavtalet och Försäkringskassans svar på Stepstones fråga om serverplacering kan kopplas till säkerhetsskyddslagen. Varken i nämnda lag eller i säkerhetsskyddsavtalet framgår att den fysiska placeringen av t.ex. en server måste vara inom Sveriges gränser. De paragrafer ur säkerhetsskyddsavtalet som kan vara aktuella vid en tolkning av detta är:

1.6 Uppdraget innebär att Leverantören i sina egna lokaler kommer att hantera och förvara uppgifter som omfattas av sekretess med hänsyn till rikets säkerhet.

Stepstone driver tjänsten i sina egna lokaler. Stepstone är ett multinationellt företag med serverhall i England och Belgien. För kundanpassade rekryteringssystem i Sverige ansvarar Stepstone Solutions AB, vilka är anbudsgi-

vare i denna upphandling och kan som svenskt företag ingå säkerhetsskyddsavtal med Försäkringskassan.

1.8 Avtalet innebär krav på att erforderligt säkerhetsskydd finns hos Leverantören med avseende på: säkerhetsskyddsorganisation, säkerhetsskyddsplan, informationssäkerhet, tillträdesbegränsning, säkerhetsprövning, utbildning och kontroll.

Av avtalet framgår inte någonting om den fysiska placeringen av servern. Punkterna ovan i avtalet kan uppfyllas även om servern inte är placerad inom Sveriges gränser.

4.4 Utländskt företag, myndighet eller medborgare får inte delges hemlig uppgift utan att Försäkringskassan lämnat Leverantören skriftligt medgivande därtill.

Försäkringskassan kan således ge medgivande utan att bryta mot säkerhetsskyddslagen. De EG-rättsliga principerna om likabehandling, proportionalitet och anti-diskriminering begränsas inte av någon nationell lagstiftning i detta fall och är således tillämpningsbara.

4.5 Personal hos Leverantören som ska ta del av hemlig uppgift ska vara behörig. Behörig att ta del av hemlig uppgift är endast den som:

- bedöms pålitlig ur säkerhetsskyddssynpunkt

- har tillräckliga kunskaper om säkerhetsskydd

- behöver uppgiften för sitt arbete i den verksamhet där hemlig uppgift förekommer.

Personalens nationalitet är således inte avgörande för behörigheten. Det torde t.o.m. vara säkrare att ha icke svenskspråkig personal för hantering av sådana uppgifter.

Stepstone anser att kravet om serverns fysiska placering är diskriminerande då det stänger ute leverantörer från andra EU-länder, samt att det strider mot den gemenskapsrättliga principen om proportionalitet då kravet är mer långtgående än vad som krävs för att uppnå syftet. Syftet med kravet måste vara att tillse en nivå av säkerhet som överensstämmer med gällande lag

och Försäkringskassans säkerhetspolicy. Försäkringskassans policy får heller inte vara begränsande för anbudsgivare utanför Sveriges gränser såvida sakligt skäl inte finns.

Försäkringskassan anför i huvudsak följande. LOU medger inga avsteg från uppställda skall-krav. Om ett skall-krav måste tas bort är den enda riktiga åtgärden att hela upphandlingen görs om - i annat fall skulle åtgärden i sig innebära ett brott mot den s.k. transparensprincipen. Skall-krav rör en upphandlings konkurrensuppsökande skede och enligt Regeringsrätten skall vid en sådan situation förordnas om att upphandlingen skall göras om. Stepstones förstahandsyrkande om rättelse skall därför inte bifallas. Försäkringskassan bestrider även Stepstones andrahandsyrkande om att upphandlingen skall göras om. Upphandlingen är korrekt genomförd och strider inte mot någon av de grundläggande principerna. Det ifrågasatta skall-kravet är proportionerligt.

Försäkringskassan har en omfattande och samhällsviktig verksamhet, varför säkerhetsskyddet är av stor betydelse. I målet aktuell upphandling omfattar ett IT-stöd för rekrytering av såväl interna som externa resurser/kompetenser, baserad på en ASP-tjänst. Anskaffningen av IT-systemet syftar till att utgöra ett stöd för HR-funktionen att planera nuvarande och framtida resurs- och kompetensbehov samt att få en bättre organiserad och ekonomiskt mer fördelaktig rekryteringsfunktion. Därför krävs att systemet har de funktioner som har efterfrågats i förfrågningsunderlaget, vilket innebär erforderligt krav på säkerhetsskydd.

Försäkringskassan lyder, med en verksamhet som anses samhällsviktig, under säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Av säkerhetsskyddslagens 5 § framgår att myndigheten skall ha det säkerhetsskydd som krävs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Enligt 6 § avses med säkerhetsskydd bl.a.

skydd av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet, vilket är aktuellt i detta fall. Säkerhetsskyddet skall enligt lagen förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet). Vidare betonas att vid utformning av informationssäkerheten skall behovet av skydd vid automatisk informationsbehandling beaktas särskilt. I 8 § åläggs myndigheten, när det i samband med den tjänst som kommer att utföras efter genomförd upphandling kommer att förekomma uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess, att träffa ett skriftligt avtal (säkerhetsskyddsavtal/SUA-avtal) med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet. Försäkringskassan har i enlighet med lagen uppställt krav på att SUA-avtal tecknas med anbudsgivaren samt beslutat att det är nödvändigt att uppställa krav på att lagring och behandling av personuppgifter skall ske i Sverige, dvs. att den server som används skall finnas och hanteras inom Sveriges gränser.

Försäkringskassan har befattningar som är säkerhetsklassade. I samband med utförande av i målet aktuell tjänst, kommer uppgifter om vilka befattningar som är säkerhetsklassade (offentlig uppgift som publiceras) samt uppgifter om vilka personer som innehar dessa befattningar att lagras och behandlas. Sammanställningen av uppgifterna om vilka personer som innehar säkerhetsklassade befattningar utgör hemlig handling enligt säkerhetsskyddsförordningen. Försäkringskassans beslut gällande sammanställningens status som hemlig handling har stämts av med säkerhetspolisen. Tillsynen avseende denna typ av beslut utövas av säkerhetspolisen.
Försäkringskassan har i enlighet med säkerhetsskyddsförordningens 5 § genomfört en säkerhetsanalys av sin verksamhet i syfte att undersöka vilka uppgifter i verksamheten som skall hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet. Försäkringskassan har vid sin bedömning och i samband

med aktuell upphandling övervägt om det finns något annat, mindre ingripande alternativ, än att ställa krav på serverns placering för att uppnå syftet med åtgärden. Försäkringskassan har inte funnit något mindre ingripande alternativ. Försäkringskassan är skyldig att löpande revidera och granska säkerheten för de system/funktioner som hanterar hemliga handlingar och har således ett långtgående ansvar för att tillse att dess leverantörer uppfyller de säkerhetskrav som har ålagts dem med anledning av uppdrag. Försäkringskassan har efter genomförd säkerhetsanalys och riskbedömning bedömt att denna inte i erforderlig mån kan säkerställa och genomföra kontroller avseende att uppställda säkerhetskrav uppfylls i det fall att servern (och således lagring och behandling av personuppgifter) placeras utanför Sveriges gränser.

Det åligger varje enskild myndighet som omfattas av berörd lagstiftning att bedöma vika säkerhetsåtgärder som är nödvändiga att vidta utifrån myndighetens verksamhet. Försäkringskassan kan endast svara för sina egna bedömningar och beslut i detta avseende. Utifrån de säkerhetsaspekter som Försäkringskassan har identifierat och grundat sitt beslut på, måste åtgärden anses vara såväl lämplig, nödvändig samt inte gå utöver vad som krävs för att uppnå syftet. Upphandlingen är korrekt genomförd och strider inte mot någon av de grundläggande principerna eller LOU.

Stepstone har i genmäle anfört bl.a. följande. Försäkringskassan påtalar att de lyder under säkerhetsskyddslagen, säkerhetsskyddsförordningen samt sekretesslagen. Försäkringskassan kan dock inte visat lagstöd för sitt absoluta krav på att server som hanterar personuppgifter av den karaktär som kan förekomma i Försäkringskassans rekryteringsverksamhet fysiskt måste vara placerad inom Sveriges gränser. I det säkerhetsskyddsavtal som leverantör skall ingå med Försäkringskassan innan uppdragets påbörjande finns ingen skrivelse om att server skall placeras inom Sveriges gränser. Försäkringskassan har inte visat hur de kom fram till att säkerheten inte kan garan-

teras om servern inte placeras i Sverige. Kontroll av säkerhetsskydd kan givetvis göras även om servern fysiskt är placerad i annat EU-land. Stepstone har ett mycket avancerat säkerhetssystem som effektivt hindrar intrång i de servrar som hanterar kundernas personuppgifter. Att bygga upp en serveranläggning i Sverige med samma säkerhetsskydd skulle kräva en betydlig investering. Ett sådant krav hindrar en sund konkurrens inom den europeiska gemenskapen och är diskriminerande. Stepstones servrar innehåller personuppgifter på mer än en miljon personer. Ingen kund har ställt som absolut krav att servern skall placeras i deras hemland, då det är helt ovidkommande för informationssäkerheten. Försäkringskassan upphandlar ett webbaserat system för rekryteringsstöd. Det är således oundvikligt att servern där personuppgifterna kommer att lagras och behandlas, oavsett vilken leverantör som erhåller uppdraget, kommer att vara tillgänglig för åtkomst över hela världen. Frågan är därför om uppgifter som rör rikets säkerhet istället borde placeras i en server som inte är uppkopplad mot Internet.

Försäkringskassan har härefter genmält bl.a. följande. Krav på serverns placering är en förutsättning för att få tillhandahålla aktuell tjänst, vilket framgår klart och tydligt av förfrågningsunderlaget. Huruvida detta stadgas i själva säkerhetsskyddsavtalet är därvid ovidkommande. Förfrågningsunderlaget kommer att utgöra en del av det avtal/upphandlingskontrakt som Försäkringskassan avser att teckna med vinnande leverantör. Försäkringskassan har i sin bedömning av behovet av säkerhetsskydd utgått från myndighetens verksamhet och den hantering av uppgifter som kommer att ske med anledning av upphandlingen. Försäkringskassan har efter genomförd säkerhetsanalys och riskbedömning bedömt att denna inte i erforderlig mån kan säkerställa och genomföra kontroller avseende att uppställda säkerhetskrav uppfylls, i det fall att servern (och således lagring och behandling av personuppgifter) placeras utanför Sveriges gränser. Försäkringskassan vill här framhålla att behovet av och sättet för genomförande av kontroller kan variera över tid. Kontroller kan exempelvis behöva ske i form av besök på

plats, kontroll av de lokaler där information/uppgifter hanteras, intervjuer, genomgång av leverantörens säkerhetsrutiner m.m. Då aspekter såsom eventuella förändringar i leverantörens verksamhet och rutiner, händelser som berör aktuell information m.m. kan påverka behovet av kontroller är det inte heller möjligt att på förhand fastställa hur frekvent och vilken typ av kontroller som kommer att behöva genomföras. Stepstone anför i sitt yttrande att kravet på serverns placering i kundens hemland är helt ovidkommande för informationssäkerheten. Försäkringskassan vill här framhålla att informationssäkerhet och säkerhetsskydd inte har samma innebörd. Informationssäkerhet tar främst sin utgångspunkt i aspekter såsom riktighet, spårbarhet, tillgänglighet, sekretess m.m., dvs. mer traditionellt skydd. Säkerhetsskydd rör rikets säkerhet och tar sin utgångspunkt i aspekter såsom terrorism, sabotage, infiltration, organiserad brottslighet m.m. Säkerhetsskydd och informationssäkerhet utgår således från vitt skilda perspektiv och syften.

DOMSKÄL

Tillämplig lagstiftning

Av 16 kap. 2 § första stycket LOU framgår bl.a. att om den upphandlande myndigheten har brutit mot de grundläggande principerna i 1 kap. 9 § eller någon annan bestämmelse i denna lag och detta har medfört att leverantören lidit eller kan komma att lida skada, skall rätten besluta att upphandlingen skall göras om eller att den får avslutas först sedan rättelse gjorts.

Enligt 1 kap. 9 § LOU skall upphandlande myndigheter behandla leverantörer på ett likvärdigt och icke-diskriminerande sätt samt genomföra upphandlingar på ett öppet sätt. Vid upphandlingar skall vidare principerna om ömsesidigt erkännande och proportionalitet iakttas.

Enligt 11 kap. 2 § LOU får en upphandlande myndighet ställa krav på en lägsta nivå för anbudssökandes och anbudsgivares ekonomiska samt tekniska och yrkesmässiga kapacitet. Dessa skall överensstämma med bestämmelserna i 7-15 §§. Omfattningen av den information som avses i 6-15 §§ samt de lägsta nivåerna för den kapacitet som krävs för ett visst kontrakt

skall ha samband med kontraktsföremålet och stå i proportion till detta. De krav på kapacitet som ställs upp skall framgå av annonsen om upphandling.

Länsrättens bedömning

Den gemenskapsrättsliga proportionalitetsprincipen skall efterlevas vid all offentlig upphandling. Prövningen i länsrätten utgör en kontroll av om det på grundval av vad sökanden har framfört i målet finns anledning att vidta sådana åtgärder som anges i 16 kap. 2 § LOU. Grund för att ingripa mot upphandlingen kan bl.a. föreligga om det visas att den upphandlande myndigheten åsidosatt de grundläggande principerna i 1 kap. 9 § LOU.

Frågan i målet är om skall-kravet i punkten 2.3.6 i bilaga B till förfrågnings-underlaget, att lagring och behandling av personuppgifter ska ske i Sverige, dvs. den server som används ska finnas och hanteras inom Sveriges gränser, är förenligt med bestämmelserna i LOU.

Det ankommer på Försäkringskassan att visa att Försäkringskassan med det uppställda skall-kravet uppnår syftet med detta (säkerhetsskydd), att syftet inte kan uppnås på ett mindre ingripande sätt samt att det föreligger balans mellan det som Försäkringskassan vinner med skall-kravet jämfört med det som de potentiella anbudsgivarna förlorar.

Försäkringskassan har hänvisat till sin egen bedömning av säkerhetskraven. Försäkringskassan har där funnit att det är nödvändigt med hänsyn till rikets säkerhet att uppställa krav på att lagring och behandling av personuppgifter skall ske i Sverige och att den server som används därför måste finnas och hanteras inom Sveriges gränser. Försäkringskassan har dock inte redogjort för sin säkerhetsbedömning. Försäkringskassan har inte heller klargjort på vilket sätt lagring och behandling av personuppgifter, inklusive den avseende de säkerhetsklassade tjänsterna vid Försäkringskassan, skulle vara mindre säker om servern placeras i annat EU-land. Någon förklaring till varför

Försäkringskassan inte i tillräcklig utsträckning kan säkerställa och genomföra kontroller av uppställda säkerhetskrav om servern placeras i annat EU-land har inte heller givits.

Länsrätten finner därför att Försäkringskassan inte visat att aktuellt skall-krav är ändamålsenligt, nödvändigt och proportionerligt i förhållande till det syfte som Försäkringskassan vill uppnå. Det uppställda skall-kravet strider därmed mot proportionalitetsprincipen.

Länsrätten finner att Stepstone har lidit eller kan komma att lida skada genom Försäkringskassans utformning av förfrågningsunderlaget. Skäl för ingripande enligt LOU föreligger därmed. Eftersom felet hänför sig till upphandlingens konkurrensuppsökande skede kan rättelse inte komma ifråga. Bolagets begäran om överprövning enligt LOU skall därmed bifallas på så sätt att upphandlingen skall göras om.

HUR MAN ÖVERKLAGAR, se bilaga (DV 3109/1a).

Marc Gren
länsrättsfiskal

Föredragande har varit Erica Nyström.

SVERIGES DOMSTOLAR

Bilaga

HUR MAN ÖVERKLAGAR - PRÖVNINGSTILLSTÅND

Den som vill överklaga länsrättens beslut skall skriva till kammarrätten i Stockholm. **Skrivelsen skall dock skickas eller lämnas till länsrätten.**

Överklagandet skall ha kommit in till länsrätten **inom tre veckor** från den dag då klaganden fick del av beslutet. Tiden för överklagandet för offentligpart räknas emellertid från den dag beslutet meddelades.

Om sista dagen för överklagandet infaller på lördag, söndag eller helgdag, midsommarafton, julafton eller nyårsafton räcker det att skrivelsen kommer in nästa vardag.

För att ett överklagande skall kunna tas upp i kammarrätten fordras att prövningstillstånd meddelas. Kammarrätten lämnar prövningstillstånd om det är av vikt för ledning av rättstillämpningen att överklagandet prövas, anledning förekommer till ändring i det slut vartill länsrätten kommit eller det annars finns synnerliga skäl att pröva överklagandet.

Om prövningstillstånd inte meddelas står länsrättens beslut fast. Det är därför viktigt att det klart och tydligt framgår av överklagandet till kammarrätten varför man anser att prövningstillstånd bör meddelas.

Skrivelsen med överklagande skall innehålla

1. den klagandes namn, personnummer, yrke, postadress och telefonnummer. Dessutom skall adress och telefonnummer till arbetsplatsen och eventuell annan plats där klaganden kan nås för delgivning lämnas om dessa uppgifter inte tidigare uppgetts i målet. Om någon person- eller adressuppgift ändras är det viktigt att anmälan snarast görs till kammarrätten,
2. det beslut som överklagas med uppgift om länsrättens namn, målnummer samt dagen för beslutet,
3. de skäl som klaganden anger till stöd för begäran om prövningstillstånd,
4. den ändring av länsrättens beslut som klaganden vill få till stånd,
5. de bevis som klaganden vill åberopa och vad han/hon vill styrka med varje särskilt bevis.

Skrivelsen skall vara undertecknad av klaganden eller hans ombud. Adressen till länsrätten framgår av beslutet. Om klaganden anlitar ombud skall denne sända in fullmakt i original samt uppge sitt namn, adress och telefonnummer.

DV 3109/1A • 2006-07 • Producerat av Domstolsverket