KONFERENSEN

INFORMATIONSSÄKERHET FÖR OFFENTLIG SEKTOR

14–15 SEPTEMBER 2016

Statens servicecenter

Att säkerställa informationssäkerhet vid upphandling

Statens servicecenter

Begrepp och definitioner

Offentlig upphandling

Offentlig upphandling innebär att en upphandlande myndighet köper, hyr eller på annat sätt anskaffar varor, tjänster eller byggentreprenader.

Upphandlande myndighet

Upphandlande myndighet kan vara myndigheter inom stat, kommuner och landsting samt kommunala eller statliga bolag eller styrelser.

Statens servicecenter

Några lagar att förhålla sig till vid upphandling

Lagen (2007:1091) om offentlig upphandling (LOU)

LOU är den lag som oftast är tillämplig. Lagen gäller för all offentlig upphandling av byggentreprenader, varor, tjänster och byggkoncessioner som inte omfattas antingen av LUF eller LUFS, eller av något specifikt undantag som är tillämpligt för den enskilda upphandlingen.

Statens servicecenter

Lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster (LUF)

LUF gäller för organisationer som bedriver verksamhet inom de angivna områdena. I vissa fall kan en upphandlande myndighet, exempelvis en kommun, bedriva verksamhet inom ramen för både LOU och LUF.

Det avgörande för vilken lag som ska tillämpas på en enskild upphandling är för vilken verksamhet det som upphandlas är avsett.

Om det som upphandlas är avsett för båda verksamheterna ska en överviktsprincip tillämpas, baserad på kontraktets värde.

Statens servicecenter

Lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS)

LUFS gäller för upphandling på försvars- och säkerhetsområdet som avser:

- militär utrustning, inklusive alla tillhörande delar, komponenter och delar av komponenter
- utrustning av känslig karaktär, inklusive alla tillhörande delar, komponenter och delar av komponenter
- byggentreprenader, varor och tjänster som direkt hänför sig till utrustningen ovan, under hela dess livslängd
- byggentreprenader och tjänster särskilt avsedda för militära syften eller byggentreprenader och tjänster av känslig karaktär.

Statens servicecenter

Offentlighets- och sekretesslag (2009:400)

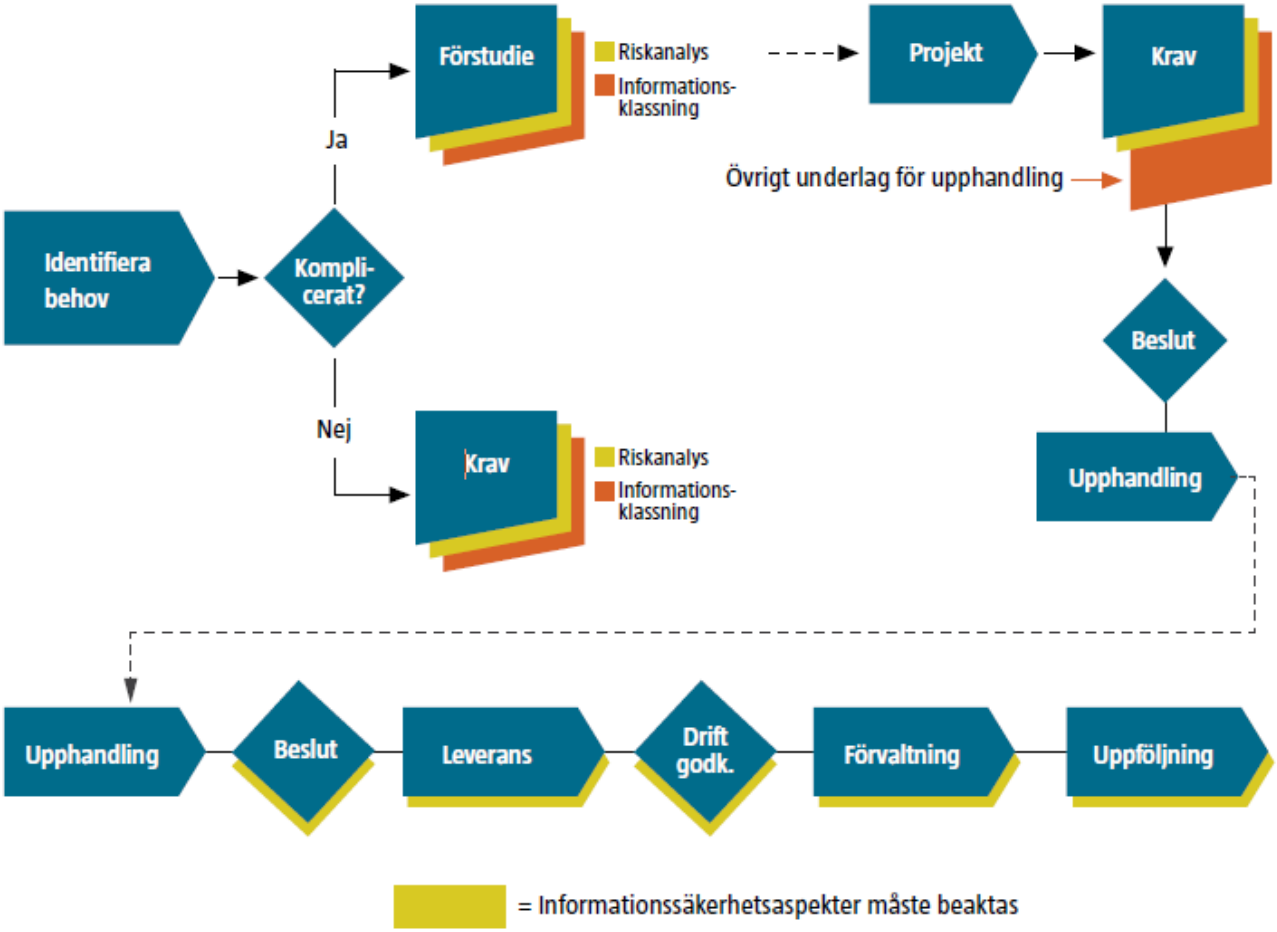
Reglerar bland annat sekretess i samband med upphandling.

Säkerhetsskyddslag (1996:627)

Reglerar bland annat krav på genomförande av säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) om det i upphandlingen förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess.

Statens servicecenter

Exempel på processbeskrivning för upphandling*



* Vägledning – Informationssäkerhet i upphandling. Myndigheten för samhällsskydd och beredskap, ISBN: 978-91-7383-338-7

Statens servicecenter

Exempel på kompetensprofiler

- Verksamhetskompetens för att identifiera krav och behov
- Säkerhetskompetens (it- och informationssäkerhet) för att bedöma risker och kunna ställa rätt säkerhetskrav
- Säkerhetsskyddskompetens vid upphandlingar som ska genomföras i form av säkerhetsskyddad upphandling med säkerhetsskyddsavtal
- It-kompetens för att göra bedömningen hur tjänsterna ska kunna integreras på lämpligt sätt i befintlig infrastruktur
- Upphandlingskompetens för att upphandlingen ska avslutas med ett affärsmässigt och verksamhetsmässigt fungerande avtal
- Juridisk kompetens för att fastställa de rättsliga förutsättningarna och kraven och se till att dessa uppfylls

Statens servicecenter

Att tänka på vid kravställning

Ta hjälp/stöd av standarder inom området

- SS-ISO/IEC 27001 och 27002 (informationssäkerhet)
- SS-EN ISO 22301 (kontinuitet)
- m.fl.

Glöm inte att ställa krav på it-incidenthantering

- Krav på myndigheter att rapportera it-incidenter följer av:
  - Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, respektive
  - Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2016:2) och allmänna råd om statliga myndigheters rapportering av it-incidenter

Försök, när så är möjligt, att ställa krav på att leverantören ska ha ett certifierat ledningssystem för informationssäkerhet – *eller likvärdigt…*

Statens servicecenter

Exempel på kravställning

Anbudssökanden ska i sin verksamhet bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet.

Ledningssystemet ska till utformning och innehåll vara i enlighet med standarderna SS-ISO/IEC 27001 och SS-ISO/IEC 27002 eller likvärdigt.

Statens servicecenter

Exempel på krav på underlag för besvarande av krav

Anbudssökande visar att kravet på ledningssystem för informations-säkerhet är uppfyllt genom att med ansökan bifoga:

- *Ett giltigt intyg om certifiering enligt SS-ISO/IEC 27001. Intyget ska vara giltigt vid tidpunkt för anbudsansökans undertecknande. Vidimerad kopia är tillräckligt.*
- *Den deklaration (så kallad Statement of Applicability, SoA) som ligger till grund för ledningssystemets innehåll och omfattning och som redovisar de kontroller i standarden som omfattas av certifieringen.*

Alternativt om likvärdigt ledningssystem (annat än SS-ISO/IEC 27001 och SS-ISO/IEC 27002) tillämpas

- *En redovisning av hur det egna ledningssystemet för informationssäkerhet är utformat, vilka säkerhetskontroller ledningssystemet omfattar, vilka av dessa säkerhetskontroller som är implementerade samt en beskrivning av hur dessa säkerhetskontroller har implementerats.*

Statens servicecenter

När upphör upphandlingen?

Upphandlingen pågår under hela avtalsperioden varför det är viktigt att säkerställa möjligheten till kontinuerlig uppföljning och kontroll av informationssäkerheten genom hela leveransen

- regelbundna samverkansmöten
- processer och rutiner för avvikelse- och incidenthantering inklusive rapportering
- möjlighet att låta genomföra inspektioner och kontroller hos leverantören – även för tredje part?

Statens servicecenter

Vägledningar och stöd

- www.informationssäkerhet.se
- Vägledning för processorienterad informationskartläggning
  Myndigheten för samhällsskydd och beredskap
- Vägledning – Informationssäkerhet i upphandling
  Myndigheten för samhällsskydd och beredskap
- Säkerhetsskyddad upphandling – En vägledning
  Säkerhetspolisen

Statens servicecenter

Slut