Nærings- og fiskeridepartementet

Forsvarsdepartementet

Veileder

Veileder om ivaretakelse av sikkerhet i offentlige anskaffelser

- sammenhenger mellom sikkerhetsloven og anskaffelsesregelverket mv.

Versjon 1

Publisert november 2019

1 Innledning

Det offentlige bruker hvert år over 500 milliarder kroner på innkjøp. Dette er offentlige midler som først og fremst skal brukes for å dekke virksomhetenes behov på en god måte, til riktig kvalitet og til lavest mulig pris. I mange anskaffelser kan det samtidig være betydelige risiko- og sikkerhetsaspekter som oppdragsgiverne må identifisere og ivareta.

Sikkerhet i offentlige anskaffelser handler blant annet om å beskytte informasjon, informasjonssystemer, objekter og infrastruktur som er omfattet av sikkerhetsloven. Dette vil være informasjon som kan skade nasjonale sikkerhetsinteresser, dersom den blir kjent for uvedkommende. Det kan også være informasjonssystemer, objekter og infrastruktur som har sentral betydning for Norges nasjonale sikkerhet.[1] I tillegg handler ivaretakelse av sikkerhet om å kunne tilby innbyggerne trygge og pålitelige tjenester, å minimere risikoen for utilsiktede hendelser og å sikre at informasjon som er gitt til det offentlige ikke kommer på avveie.

Bruk av ny teknologi og nye løsninger gir nye sårbarheter og et stadig endret sikkerhetsrisikobilde. Infrastrukturer og IKT-systemer blir mer komplekse, globale og integrerte. Flere enheter kobles til internett, og bruk av skyløsninger øker. Behovet for å redusere kostnader og øke tilgangen til kompetanse gjør at flere IKT-funksjoner settes ut til private leverandører.

Nasjonal sikkerhetsmyndighet (NSM) registrerer daglig at norske virksomheter blir utsatt for uønskede digitale hendelser, i form av for eksempel nettverksoperasjoner hvor virksomhetenes informasjonssystemer blir forsøkt kompromittert. Noen av disse hendelsene er alvorlige, og NSM vurderer at de mest alvorlige sakene nå er mer omfattende og mer komplekse enn tidligere.[2] NSM peker også på at offentlige virksomheter, både sivile og militære, i økende grad blir avhengige av privat sektor, og at næringslivet i enda større grad vil levere tjenester og utstyr til sektorer av betydning for Norge i fremtiden.[3] Det er dermed viktig at aktørene, både offentlige og private, forstår

[1] Informasjonssikkerhet, informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet er forhold som er omfattet av sikkerhetsloven, jf. sikkerhetsloven kapittel 5 til 7.

[2] Se NSMs rapport "Risiko 2019 – Krafttak for et sikrere Norge", s. 10.

[3] Se NSMs rapport "Risiko 2019 – Krafttak for et sikrere Norge", s. 20.

hvilke risikoer de forvalter og at disse risikoene håndteres på en god måte gjennom risikoreduserende tiltak.

Regjeringens overordnede mål er at norske virksomheter digitaliserer på en sikker og tillitsvekkende måte, med bedre evne til egen beskyttelse mot uønskede digitale hendelser, samt at kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur.[4] Gode offentlige anskaffelser, som setter krav til ivaretakelse av sikkerhet, er viktig for å nå disse målsettingene.

Formålet med denne veilederen er todelt. Veilederen skal vise sammenhenger mellom reglene i sikkerhetsloven og reglene i anskaffelsesregelverket, og veilederen skal også synliggjøre de mulighetene for å ivareta sikkerhet som ligger i anskaffelsesregelverket. Veilederen har som mål å synliggjøre handlingsrommet i anskaffelsesregelverket, og gjennom dette hvordan oppdragsgiverne kan ivareta norske sikkerhetsinteresser i møte med leverandører med tilknytning til stater som vi ikke har et sikkerhetsmessig samarbeid med.

I anskaffelser hvor sikkerhet er et sentralt element, er det ofte flere regelverk som virker i sammenheng. For eksempel vil sikkerhetsloven i mange tilfeller virke i tillegg til reglene i den aktuelle forskriften på anskaffelsesområdet. I kapittel 2 viser vi sammenhenger mellom regelverkene, og da særlig hvordan de materielle reglene i sikkerhetsloven virker i samsvar med prosedyrereglene i anskaffelsesregelverket. Hvilke leverandører som er rettighetshavere etter anskaffelsesregelverket, følger av internasjonale avtaler Norge er forpliktet av. I kapittel 2 gis det også en oversikt over hvem som er rettighetshavere etter anskaffelsesregelverket.

For å kunne ivareta sikkerhet på en god måte, må oppdragsgiverne ha god forståelse av risikoene den aktuelle anskaffelsen innebærer. Risikovurderinger i forkant av anskaffelsen er omtalt i kapittel 3. Slike risikovurderinger danner utgangspunktet for videre krav til ivaretakelse av sikkerhet.

---

[4] Målene fremgår av Nasjonal strategi for digital sikkerhet, hvor offentlig privat samarbeid trekkes frem som et prioritert område. Strategien er tilgjengelig på Justis- og beredskapsdepartementets nettsider. Også eForvaltningsforskriften pålegger forvaltningsorganer å ha mål og strategi for informasjonssikkerhet som skal danne grunnlaget for forvaltningsorganets internkontroll på informasjonssikkerhetsområdet.

I enkelte anskaffelser foreligger det tungtveiende sikkerhetshensyn som ikke er forenelig med prosedyrene i regelverket. Disse anskaffelsene kan derfor unntas fra anskaffelsesregelverket. Unntaksadgangen er nærmere omtalt i kapittel 4.

Samtidig gir anskaffelsesforskriften, forsyningsforskriften og konsesjonskontraktsforskriften en rekke muligheter til å stille krav og sette kriterier knyttet til ivaretakelse av sikkerhet, også for anskaffelser som ikke er underlagt sikkerhetsloven. I kapittel 5 vil vi se nærmere på adgangen til å stille krav til ivaretakelse av sikkerhet etter anskaffelsesforskriften mv. I dette kapitlet går vi blant annet inn på mulighetene for testing av leveransen.

Forsvarsdepartementet har utarbeidet en veileder til forskrift om forsvars- og sikkerhetsanskaffelser. I tillegg arbeider NSM med en veileder til sikkerhetsgraderte anskaffelser etter sikkerhetsloven. Det vises til disse veilederne i kapittel 2.

I en del tilfeller vil det oppstå konkrete problemstillinger hvor det ikke er mulig, eller hensiktsmessig, å ta stilling til spørsmålet på forhånd i en generell veileder. I slike tilfeller er det viktig at oppdragsgiverne tilknytter seg den nødvendige sikkerhetsfaglige kompetansen på det aktuelle området.

I mange lover og forskrifter stilles det krav til sikkerhet ut over det som følger av sikkerhetsloven, og som oppdragsgiverne må være oppmerksomme på i sine anskaffelser. For eksempel stilles det krav til informasjonssikkerhet ved behandling av personopplysninger etter personopplysningslovgivningen. I denne veilederen går vi ikke nærmere inn på spesifikke sikkerhetskrav i annen lovgivning.

Departementet gjør oppmerksom på at det er domstolene som har det avgjørende ordet ved tolkningen av anskaffelsesreglene. Vurderingene i veilederen er derfor kun rådgivende.

2 Sammenheng mellom de ulike regelverkene

2.1 Generelt

Det er flere regelverk oppdragsgiverne må ta hensyn til ved ivaretakelse av sikkerhet i anskaffelser.

Anskaffelsesloven med tilhørende forskrifter (**anskaffelsesregelverket**) gjelder når det offentlige inngår vare-, tjeneste- og bygge- og anleggskontrakter med en anslått verdi som er lik eller overstiger 100 000 kroner. Regelverket er et prosedyreregelverk som inneholder grunnleggende prinsipper og krav til prosedyrer som må følges ved offentlige innkjøp.

De fire sentrale forskriftene i anskaffelsesregelverket er:

- **Anskaffelsesforskriften**: Forskrift om offentlige anskaffelser regulerer de ordinære anskaffelsene. Nærings- og fiskeridepartementet har utarbeidet en veileder til anskaffelsesforskriften.
- **Forsyningsforskriften**: Forskrift om innkjøpsregler i forsyningssektorene regulerer anskaffelser knyttet til utøvelsen av visse forsyningsaktiviteter (innenfor gass og varme, elektrisitet, drikkevann, transport, havner og lufthavner, post, olje gass, kull og andre typer brensel). Nærings- og fiskeridepartementet har utarbeidet veileder om virkeområdet for forsyningsforskriften.
- **Konsesjonskontraktforskriften**: Forskrift om konsesjonskontrakter regulerer anskaffelser der kontraktstypen er en konsesjonskontrakt. Nærings- og fiskeridepartementet har utarbeidet en overordnet veileder til konsesjonskontraktforskriften.
- **Forskrift om forsvars- og sikkerhetsanskaffelser:** Forskrift om forsvars- og sikkerhetsanskaffelser (FOSA) regulerer visse anskaffelser på forsvars- og sikkerhetsområdet. Forsvarsdepartementet har utarbeidet en veileder til FOSA.

Mange av anskaffelsene på sikkerhetsområdet omfattes av FOSAs virkeområde, og skal derfor følge anskaffelsesloven og FOSA.[5] Anskaffelsesforskriften er negativt avgrenset mot de øvrige prosedyreforskriftene, herunder FOSA. [6]

---

[5] Hvilke kontrakter som er omfattet av FOSAs virkeområde er nærmere omtalt i kapittel 6 i veilederen til FOSA.

[6] Det fremgår av anskaffelsesforskriften § 2-1 at forskriften ikke gjelder for anskaffelser knyttet til utøvelsen av forsyningsaktiviteter, anskaffelser på forvars- og sikkerhetsområde som definert i forskrift om forsvars- og sikkerhetsanskaffelser § 1-3 første ledd eller for konsesjonskontrakter.

I tillegg stiller **sikkerhetsloven** med tilhørende forskrifter (heretter "sikkerhetsloven") særlige krav til hvordan oppdragsgivere og leverandører må ta hensyn til sikkerhet i anskaffelser. Nasjonal sikkerhetsmyndighet har utarbeidet flere veiledere til sikkerhetsloven.

En anskaffelse kan både være underlagt anskaffelsesregelverket og sikkerhetsloven. En anskaffelse kan for eksempel være underlagt prosedyrereglene i FOSA eller forsyningsforskriften, og sikkerhetsreglene i sikkerhetsloven.

Eksempel

Politiet skal kjøpe kryptert radioutstyr. I forbindelse med anskaffelsen kan leverandøren få tilgang til sikkerhetsgradert informasjon. Denne anskaffelsen skal følge både prosedyrereglene i FOSA og krav til sikkerhet i sikkerhetsloven.

Eksempel

En kommune skal anskaffe alarmtjenester til et vannverk i kommunen. Vannverket er identifisert som skjermingsverdig objekt eller infrastruktur, med klassifisering som KRITISK. Leverandøren vil få elektronisk tilgang fra sine egne informasjonssystemer til overvåkningsbilder og få mulighet til å skru av alarmen i oppdragsgivers lokaler. Denne anskaffelsen skal følge prosedyrereglene i forsyningsforskriften og krav til sikkerhet i sikkerhetsloven. . I dette tilfellet skal oppdragsgiveren, i tillegg til å stille krav om sikkerhetsavtale, stille krav om leverandørklarering, da leverandøren vil få elektronisk tilgang til objekt eller infrastruktur som er klassifisert som KRITISK.

Samtidig er det viktig å være oppmerksom på at virkeområdene til anskaffelsesregelverket og sikkerhetsloven ikke er overlappende. Det vil si at sikkerhetsloven kan stille krav som oppdragsgiverne må ta hensyn til i en anskaffelse, selv om den ikke er underlagt anskaffelsesregelverket. En anskaffelse kan for eksempel være omfattet av sikkerhetsloven, men unntatt fra anskaffelsesregelverket etter EØS-avtalen artikkel 123.

Det kan også være tilfeller der det er nødvendig å stille krav til sikkerhet ved gjennomføringen av en anskaffelse etter anskaffelsesregelverket, selv om det ikke er påkrevd etter sikkerhetsloven. Eksempelvis kan det stilles krav til sikkerhet for ivaretakelse av taushetsbelagte opplysninger i en alminnelig it-anskaffelse.

Det kan også være anskaffelser der det er nødvendig å stille krav til sikkerhet som ikke er påkrevd etter sikkerhetsloven, og hvor anskaffelsen heller ikke er underlagt anskaffelsesregelverket. Eksempelvis kan det stilles krav til sikkerhet for ivaretakelse av personopplysninger i en kontrakt om en forsknings- og utviklingstjeneste som er unntatt anskaffelsesregelverket.

2.2 Krav til sikkerhet etter sikkerhetsloven i en anskaffelsesprosess

Sikkerhetsloven er en rammelov som regulerer forebyggende sikkerhetsarbeid i virksomheter av betydning for nasjonal sikkerhet.[7] Ny sikkerhetslov med nye forskrifter, herunder forskrift om virksomheters arbeid med sikkerhet (virksomhetsikkerhetsforskriften) og forskrift om sikkerhetsklarering og annen klarering (klareringsforskriften), trådte i kraft 1. januar 2019.[8]

Formålet med den nye sikkerhetsloven er, i likhet med den tidligere sikkerhetsloven, å trygge nasjonale sikkerhetsinteresser, og særlig landets suverenitet, territorielle integritet og demokratiske styreform. Den nye sikkerhetsloven er innrettet for å beskytte de sentrale samfunnsfunksjonene som understøtter disse interessene. Disse funksjonene er kalt grunnleggende nasjonale funksjoner.

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer, og for leverandører av varer og tjenester i forbindelse med sikkerhetsgraderte anskaffelser.[9] Departementene skal innenfor sine ansvarsområder treffe vedtak om at andre virksomheter underlegges loven dersom de behandler sikkerhetsgradert informasjon eller råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller driver aktivitet som

[7] Foruten sikkerhetsloven kommer beskyttelsesinstruksen til anvendelse ved behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i sikkerhetsloven med forskrifter, jf. beskyttelsesinstruksen § 1.

[8] Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven). Sikkerhetsloven avløste lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

[9] Sikkerhetsloven § 1-2.

har avgjørende betydning for disse funksjonene.[10] Denne innretningen innebærer at den nye sikkerhetsloven har et noe videre virkeområde enn den gamle loven.

De fleste oppdragsgiverne som er underlagt anskaffelsesregelverket, er også underlagt sikkerhetsloven. Det er likevel ikke slik at alle oppdragsgivere som er underlagt anskaffelsesregelverket automatisk er omfattet av sikkerhetsloven. Sikkerhetsloven gjelder for eksempel ikke direkte for alle offentligrettslige organer, eller for alle offentlige foretak eller andre virksomheter som utøver forsyningsaktivitet på grunnlag av enerett eller særrett. Departementene kan imidlertid fatte vedtak om at slike virksomheter skal underlegges sikkerhetsloven. Det er også slik at ikke alle oppdragsgivere som potensielt underlegges sikkerhetsloven, må følge anskaffelsesregelverket. Departementene kan fatte vedtak om at virksomheter som ikke er oppdragsgivere etter anskaffelsesregelverket, underlegges sikkerhetsloven.

Sikkerhetsloven stiller en rekke særegne krav til sikkerhet som det er viktig å være oppmerksom på i en anskaffelsesprosess. Hvilke krav i sikkerhetsloven og tilhørende forskrifter som gjelder for oppdragsgiverne, vil avhenge av hvilken skjermingsverdig informasjon, eller hvilke type skjermingsverdige informasjonssystemer, infrastruktur eller objekter virksomhetene råder over, eller skal være i stand til å behandle. Hvilke krav som gjelder i forbindelse med anskaffelsen, vil avhenge av hva leverandøren eller personell fra leverandøren får tilgang til.

Sikkerhetslovens krav til sikkerhet, herunder krav til sikkerhetsavtale, leverandørklarering og personellklarering, må ivaretas i anskaffelsesprosessen. Etter anskaffelsesregelverket kan oppdragsgivere stille krav til leverandørene om beskyttelse av informasjon av fortrolig karakter som gjøres tilgjengelig for dem i forbindelse med en anskaffelse.[11][12] På hvilket tidspunkt i anskaffelsen kravene må oppfylles, avhenger av

---

[10] Sikkerhetsloven § 1-3.

[11] Jf. anskaffelsesforskriften § 7-4. Om dette, se Arrowsmith, Sue, The law of Public and Utilities procurement – Regulation in the EU and the UK, 3. utg. Volum 1, London: Sweet & Maxwell, 2014, (Arrowsmith Vol 1), side 635-636.

[12] I FOSA er det i tillegg flere bestemmelser som eksplisitt gir oppdragsgivere mulighet til å stille krav til sikkerhet i forbindelse med sine anskaffelser. Disse bestemmelsene er nærmere omtalt i veielderen til FOSA, særlig kapittel 13.9. Om forholdet mellom anskaffelsesdirektivet og direktivet om forsvars- og sikkerhetsanskaffelser, se Arrowsmith, Sue, The law of Public and Utilities procurement – Regulation in the EU and the UK, 3. utg. Volum 2, London: Sweet & Maxwell, 2018, (Arrowsmith Vol 2) s. 242.

når leverandøren eller personellet får tilgang til skjermingsverdig informasjon, informasjonssystem, infrastruktur eller objekt.

Der oppdragsgivere stiller krav til sikkerhet etter sikkerhetsloven, må dette fremgå av konkurransegrunnlaget. Det er flere måter oppdragsgivere kan stille krav til sikkerhet på i en anskaffelsesprosess. I mange tilfeller kan anskaffelsen struktureres slik at det kun er nødvendig å gi valgte leverandør tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur i kontraktsgjennomføringen. I slike tilfeller kan kravene til sikkerhet stilles som en forutsetning for kontraktsinngåelse eller som kontraktsvilkår.

Der krav til sikkerhet stilles som en forutsetning for kontraktsinngåelse, bør oppdragsgiver være oppmerksom på at det kan ta tid å oppfylle kravene til sikkerhet i sikkerhetsloven, for eksempel krav om leverandørklarering. Dette bør oppdragsgivere hensynta ved fastsettelsen av vedståelsesfristens lengde, slik at oppdragsgivere har mulighet til å endre tildelingsbeslutningen dersom det viser seg at valgte leverandør ikke oppfyller de nødvendige sikkerhetskravene.

I enkelte anskaffelser vil det imidlertid være behov for å stille krav til sikkerhet før valg av leverandør. For eksempel kan det være slik at deler av konkurransegrunnlaget inneholder sikkerhetsgradert informasjon som ikke kan gis ut *før* kravene til sikkerhet er oppfylt. I så fall må interesserte eller prekvalifiserte tilbydere oppfylle kravene til sikkerhet, før de får tilstrekkelig informasjon til å inngi tilbud. I slike tilfeller kan det være hensiktsmessig å gjennomføre en prekvalifisering for å redusere antall leverandører. I planleggingsfasen må oppdragsgivere alltid vurdere om det er nødvendig at konkurransegrunnlaget inneholder sikkerhetsgradert informasjon. Både for oppdragsgiveren og leverandørene, kan det være tid- og ressurskrevende å oppfylle kravene til sikkerhet etter sikkerhetsloven.

Nedenfor gis det en overordnet fremstilling av de mest sentrale kravene for anskaffelser etter sikkerhetsloven.

2.2.1 Sikkerhetsgraderte anskaffelser

I sikkerhetsloven er det egne regler om sikkerhetsgraderte anskaffelser. NSM arbeider med en egen veileder om dette.

Sikkerhetsgradert anskaffelse

En sikkerhetsgradert anskaffelse er en anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, eller få tilgang til et skjermingsverdig objekt eller infrastruktur.[13]

Med *leverandøren* menes i denne sammenheng alle tilbydere, leverandører og underleverandører i en anskaffelse.

Sikkerhetsgradert informasjon er informasjon som kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende[14]. Virksomheter som tilvirker slik informasjon skal sikkerhetsgradere og merke slik informasjon. I sikkerhetsloven brukes det ulike sikkerhetsgrader: STRENGT HEMMELIG, HEMMELIG, KONFIDENSIELT og BEGRENSET.

Objekter og infrastruktur er skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. [15] Departementene skal innenfor sine ansvarsområder utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur. I sikkerhetsloven brukes det ulike klassifiseringsgrader; MEGET KRITISK, KRITISK og VIKTIG.

For sikkerhetsgraderte anskaffelser stilles det i sikkerhetsloven kapittel 9 krav til sikkerhetsavtale med leverandørene, leverandørklarering og varslingsplikt til myndighetene. Ved sikkerhetsgraderte anskaffelser er det også viktig å være klar over reglene om personellsikkerhet i sikkerhetslovens kapittel 8. Nedenfor gis det en kort presentasjon av disse kravene og hvordan de inngår i en anskaffelsesprosess.

[13] Sikkerhetsloven § 9-1.

[14] Sikkerhetsloven § 5-3.

[15] Sikkerhetsloven § 7-1.

Sikkerhetsavtale

Før en sikkerhetsgradert anskaffelse iverksettes, skal oppdragsgiveren inngå en sikkerhetsavtale med leverandøren. Sikkerhetsavtalen skal tydeliggjøre og konkretisere partenes plikter og ansvar etter sikkerhetsloven.

Sikkerhetsavtalen skal alltid inneholde hvilken sikkerhetsgrad anskaffelsen skal ha, spesifisert for hver del av oppdraget, og hvordan leverandøren skal forholde seg til de av lovens krav som gjelder for anskaffelsen. For de tilfeller der leverandøren skal ha tilgang til informasjon, objekt eller infrastruktur fra sine egne lokaler, stilles det egne krav til sikkerhetsavtalen i virksomhetsikkerhetsforskriften.[16]

Virksomhetsikkerhetsforskriften gir også et praktisk unntak for krav til sikkerhetsavtale for de tilfeller der leverandørens personell bare skal gis tilgang til informasjon, objekt eller infrastruktur under oppsyn av en representant for oppdragsgiveren.[17]

En sikkerhetsavtale må inngås før en sikkerhetsgradert anskaffelse *iverksettes,* det vil si før leverandøren av varen eller tjenesten kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, eller får tilgang til et skjermingsverdig objekt eller infrastruktur. I anskaffelser der tilbydere kan få tilgang til slik informasjon, objekt eller infrastruktur i konkurransefasen, må det følgelig inngås sikkerhetsavtale med samtlige tilbydere. Der det kun gis tilgang til slik informasjon, objekter eller infrastruktur i kontraktsgjennomføringsfasen, er det tilstrekkelig at det inngås sikkerhetsavtale med valgte leverandør.

Leverandørklarering

Ved sikkerhetsgraderte anskaffelser, er det alltid krav om leverandørklarering dersom leverandøren skal

- ha tilgang til eller oppbevare informasjon gradert KONFIDENSIELT eller høyere i sine egne informasjonssystemer eller lokaler
- ha elektronisk tilgang fra sine egne informasjonssystemer eller lokaler til objekter eller infrastruktur klassifisert KRITISK eller MEGET KRITISK

[16] Jf. virksomhetsikkerhetsforskriften § 80.

[17] Jf. virksomhetsikkerhetsforskriften § 81.

- råde over objekter eller infrastruktur som tilhører oppdragsgiveren, og som er klassifisert. [18]

Leverandøren skal også ha leverandørklarering når det av andre grunner er nødvendig for å oppnå et forsvarlig sikkerhetsnivå i anskaffelsen.[19]

Formålet med leverandørklareringen er å kontrollere at leverandøren er i stand til oppfylle kravene i sikkerhetsloven som gjelder behandlingen av den graderte informasjonen leverandøren skal ha tilgang til, eller kravene som gjelder for tilgangen til det aktuelle skjermingsverdige informasjonssystemet, objektet eller infrastrukturen.

Forespørsel om leverandørklarering rettes til klareringsmyndigheten for leverandører, i praksis vil det si NSM.[20] Vurderingsgrunnlaget for leverandørklarering og hvilke kilder klareringsmyndigheten kan basere leverandørklareringen på, er nærmere fastsatt i klareringsforskriften.[21]

Leverandørene skal klareres *før* leverandørene får tilgang til informasjonen, objektet eller infrastrukturen. Om tilbyderne får slik tilgang i konkurransegjennomføringsfasen, må det følgelig innhentes leverandørklarering fra samtlige tilbydere. Der det kun gis slik tilgang i kontraktsgjennomføringsfasen, er det tilstrekkelig med leverandørklarering av valgte leverandør. I planleggingsfasen, bør oppdragsgiverne være oppmerksomme på det kan ta tid å innhente leverandørklarering. NSM bruker normalt tre måneder på å behandle en forespørsel om leverandørklarering.

Personellsikkerhet

I tillegg til krav om sikkerhetsavtale, leverandørklarering og varslingsplikt må også sikkerhetsloven og forskriftens krav til personellsikkerhet følges ved sikkerhetsgraderte anskaffelser. [22] NSM har utarbeidet en veileder i personellsikkerhet.

---

[18] Virksomhetsikkerhetsforskriften § 83.

[19] Krav om leverandørklarering fremgår av sikkerhetsloven § 9-3 og virksomhetsikkerhetsforskriften §83.

[20] Virksomhetsikkerhetsforskriften § 85.

[21] Se klareringsforskriften §§ 33-35.

[22] Sikkerhetsloven kapittel 8.

Personer som skal få tilgang til sikkerhetsgradert informasjon, skal autoriseres og eventuelt sikkerhetsklareres.[23] Alle personer som skal få tilgang til sikkerhetsgradert informasjon, skal autoriseres. Kravet gjelder for alle graderingsnivåer, det vil si for informasjon som er gradert BEGRENSET og oppover. Virksomhetens leder er autorisasjonsansvarlig.[24] I tillegg må personer som skal eller kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, ha gyldig sikkerhetsklarering.[25] Personer som skal ha adgang til skjermingsverdige objekter eller infrastruktur, skal autoriseres dersom det er fattet vedtak om krav til adgangsklarering. Sikkerhetsklarering og adgangsklarering gjøres av klareringsmyndigheten.[26]

Om leverandørenes personell må sikkerhetsklareres eller adgangsklareres i konkurransegjennomføringsfasen, må klarering innhentes fra de aktuelle personene hos samtlige tilbydere. Dersom klarering av personell kun er nødvendig ved kontraktsgjennomføringen, er det tilstrekkelig å innhente klarering fra det aktuelle personellet hos valgte leverandør. Oppdragsgiveren må være klar over at det kan ta tid å innhente sikkerhetsklarering og adgangsklarering, og ta hensyn til dette ved planleggingen av sine anskaffelser. En klareringsavgjørelse vil normalt ta fire uker, men avhengig av den konkrete saken vil det kunne gå noe lengre tid. I saker hvor det må søkes om klarering for utenlandske statsborgere vil det kunne ta vesentlig lengre tid, avhengig av hvilken stat den aktuelle personen kommer fra.

Utenlandske leverandører

Dersom en utenlandsk leverandør eller dennes personell må klareres eller gis tilgang til sikkerhetsgradert informasjon, skal sikkerhetsmyndigheten godkjenne leverandøren før det inngås en sikkerhetsavtale.[27] En utenlandsk leverandør er i denne sammenheng en leverandør som driver virksomheten sin fra en annen stats jurisdiksjon, eller skal behandle eller oppbevare informasjon i lokaler utenfor norsk jurisdiksjon. Bakgrunnen for kravet er at klareringsmyndighetene og/eller sikkerhetsmyndigheten (NSM), ikke har

[23] Sikkerhetsloven § 8-1.

[24] Sikkerhetsloven § 8-9.

[25] Sikkerhetsloven § 8-2.

[26] Sikkerhetsloven § 8-4.

[27] Sikkerhetsloven § 9-2.

jurisdiksjon til å kontrollere leverandøren eller tilgang til de registrene som er nødvendig for å klarere personer fra leverandøren i disse tilfellene.

Hva godkjenningen innebærer, vil avhenge av om den utenlandske leverandøren skal ha tilgang til informasjonen fra egne lokaler eller om personer fra leverandøren skal ha tilgang til informasjonen i oppdragsgivers lokaler. Skal personene fra leverandøren ha tilgang til informasjonen i oppdragsgivers lokaler, skal personene være klarert, og godkjenningen vil innebære en kontroll av om personene har tilstrekkelig klarering. Har personene en klarering fra hjemstaten kan denne legges til grunn for tilgang til norsk sikkerhetsgradert informasjon, dersom Norge har et sikkerhetssamarbeid med hjemstaten som også omfatter klarering. I disse tilfellene vil godkjenningen innebære at NSM tar kontakt med sikkerhetsmyndigheten i hjemstaten og ber om en bekreftelse på at vedkommende er klarert. Innhenting av en slik bekreftelse vil normalt ta fem virkedager, og godkjenningen av sikkerhetsavtalen vil da kunne foreligge innen relativt kort tid.

Har ikke personen klarering, må NSM enten ta kontakt med sikkerhetsmyndigheten i hjemstaten og be om at det gjennomføres en klareringsprosess der, eller så må NSM selv gjøre en klarering etter reglene om klarering av utenlandske statsborgere, jf. sikkerhetsloven § 8-7 med tilhørende forskriftsbestemmelser. Hvilken prosess som velges avhenger av det sikkerhetsmessige samarbeidet med det aktuelle landet. Uansett vil godkjenningen av sikkerhetsavtalen ta lengre tid enn i de tilfellene hvor personen allerede har klarering fra tidligere.

Dersom den utenlandske leverandøren skal leverandørklareres, vil godkjenningen av sikkerhetsavtalen sammenfalle med leverandørklareringen.[28] Har leverandøren klarering fra hjemstaten, vil den kunne legges til grunn for tilgang til norsk sikkerhetsgradert informasjon, dersom Norge har et sikkerhetssamarbeid med hjemstaten som omfatter leverandørklarering. I disse tilfellene vil godkjenningen innebære at NSM tar kontakt med sikkerhetsmyndigheten i hjemstaten og ber om en bekreftelse på at leverandøren er klarert i hjemstaten.

Dersom leverandøren ikke er klarert, må NSM enten ta kontakt med sikkerhetsmyndigheten i hjemstaten og be om at det gjennomføres en leverandørklarering der, eller så må NSM selv gjennomføre en leverandørklareringsprosess. NSM er da avhengig av å få tilgang til nødvendige opplysninger fra den andre staten, noe som forutsetter et sikkerhetssamarbeid.

[28] Sikkerhetsloven § 9-3.

Skal den utenlandske leverandøren ha tilgang til sikkerhetsgradert informasjon gradert BEGRENSET fra sine lokaler, skal også NSM godkjenne sikkerhetsavtalen. For nærmere om godkjenningsprosessen i disse tilfellene, se NSMs kommende veileder.

Varslingsplikt

Ved anskaffelser til skjermingsverdig informasjonssystem,[29] objekt eller infrastruktur skal oppdragsgiveren *vurdere* om anskaffelsen kan innebære en ikke ubetydelig risiko for at informasjonssystemet, objektet eller infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet, og hvordan risikoen skal håndteres.[30] Oppdragsgiveren skal *varsle* overordnet departementet dersom vurderingen viser at anskaffelsen innebærer en slik ikke ubetydelig risiko.[31] Oppdragsgiverne må ta hensyn til disse pliktene tidlig i planleggingen av anskaffelsene sine.

Plikten til å foreta en slik vurdering gjelder ikke dersom anskaffelsen åpenbart ikke innebærer en slik risiko. Plikten til å varsle gjelder ikke dersom oppdragsgiveren selv iverksetter tiltak som fjerner risikoen eller gjør den ubetydelig. Dersom en anskaffelse til et skjermingsverdig informasjonssystem, objekt eller infrastruktur kan innebære en ikke ubetydelig risiko som nevnt i første ledd, kan Kongen i statsråd fatte vedtak om at anskaffelsen ikke skal gjennomføres, eller at det skal settes vilkår for den.

2.3 Rettighetshavere

Foruten norske leverandører har også leverandører som er gitt rettigheter etter internasjonale avtaler som Norge har på anskaffelsesområdet, rettigheter etter anskaffelsesloven og tilhørende forskrifter.[32] Disse leverandørene har krav på å bli behandlet likt med norske leverandører i konkurranser om offentlige anskaffelser, og har adgang til å klage til Klagenemda for offentlige anskaffelser (KOFA) og til domstolene hvis de mener det foreligger brudd på anskaffelsesregelverket.

---

[29] Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner, jf. sikkerhetsloven § 6-1.

[30] Virksomhetsikkerehtsforskriften § 18.

[31] Sikkerhetsloven § 9-4 og virksomhetsikkerhetsforskriften § 19.

[32] Anskaffelsesloven § 3.

Utenlandske leverandører som har rettigheter etter anskaffelsesregelverket kan deles inn i tre grupper:

- leverandører fra EØS-stater
- leverandører som er gitt rettigheter etter WTO-avtalen om offentlige innkjøp (GPA)
- leverandører som er gitt rettigheter etter andre internasjonale avtaler som Norge er forpliktet av, det vil si bilaterale avtaler som dekker offentlige anskaffelser.

I hvilken utstrekning leverandører fra land vi har internasjonale avtaler med er rettighetshavere etter anskaffelsesregelverket, er nærmere omtalt i Nærings- og fiskeridepartementets veileder om rettighetshavere. Europakommisjonen har også publisert veiledning om leverandører fra tredjeland, og hvordan oppdragsgiver kan stille krav for å oppnå like konkurransevilkår når slike leverandører gis adgang til å inngi tilbud.[33]

Utenlandske leverandører som ikke er rettighetshavere, kan utelukkes fra konkurransen uten annen begrunnelse enn at leverandøren ikke er rettighetshaver. Problemstillinger spesifikt knyttet til leverandører fra land som Norge ikke har avtalemessig tilknytning til på anskaffelsesområdet, vil ikke bli behandlet nærmere i denne veilederen.

[33] Se Europakommisjonen *Guidance on the participation of third country bidders and goods in the EU procurement market*.

3 Risikovurdering i forkant av anskaffelsen

En anskaffelsesprosess består av flere faser der oppdragsgiverne må foreta ulike vurderinger og beslutninger for å sikre at anskaffelsen både gir god behovsdekning og at den blir gjennomført i henhold til lover og regler. Planleggingsfasen, som er første del av anskaffelsesprosessen, består i hovedsak av å avklare behovet, legge en plan og forberede gjennomføringen av konkurransen.

I planleggingsfasen er det også viktig å vurdere hvilke regelverk som må tas i betraktning i forbindelse med anskaffelsen, herunder om det finnes regelverk som stiller krav til risikovurdering og risikostyring for den aktuelle anskaffelsen. For eksempel stilles det krav til risikostyring etter sikkerhetsloven. Risikovurderinger etter sikkerhetsloven er nærmere beskrevet i NSMs veileder i sikkerhetsstyring.

I anskaffelser der sikkerhet er et sentralt element, men hvor anskaffelsen ikke er underlagt sikkerhetsloven eller FOSA, er det også viktig å vurdere konkret hvilke risikoer anskaffelsen vil innebære. Nedenfor gis noen utgangspunkter for gjennomføring av risikovurderinger i anskaffelser som ikke er underlagt sikkerhetsloven eller FOSA.

Forvaltningsorganer er gjennom eForvaltningsforskriften pålagt å ha internkontroll på informasjonssikkerhetsområdet.[34] Internkontrollen skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Disse standardene forutsetter tilstrekkelig risikostyring i virksomheten, herunder at risiko vurderes i forkant av IKT-anskaffelser. Omfanget på risikovurderingen må tilpasses oppdragsgiverens antakelser om risikoen som foreligger.

Gjennom risikovurderinger skal oppdragsgiverne identifisere mulige sikkerhetsrisikoer knyttet til verdiene anskaffelsen er relatert til, samt identifisere blant annet trusler og mulige konsekvenser for virksomheten ved et sikkerhetsbrudd. Deretter må risikoene analyseres og evalueres. Arbeidet med identifisering av risiko bør utføres i samarbeid mellom personer som kjenner det aktuelle fagområdet godt og personer som har kompetanse på sikkerhet.

Identifiseringen skal lede til en oversikt over relevante sikkerhetsrisikoer knyttet til anskaffelsen. Dette kan gjennomføres som en idémyldring over hvilke uønskede hendelser som kan oppstå, hvilke sikkerhetsbrudd som kan tenkes og hvilke konsekvenser hendelsene kan føre til.

[34] eForvaltningsforskriften § 15.

Risikoanalysen har som mål å analysere hver enkelt risiko og estimere omfanget av konsekvensene, med tilhørende sannsynlighet, for så å fastsette et samlet risikonivå for anskaffelsen. Det er ofte vanlig å skille mellom lav, moderat, høy og svært høy risiko.

Evalueringen skal ta stilling til hvilke risikoer som kan aksepteres som de er, og hvilke risikoer som krever nærmere håndtering. I evalueringen skal risikoene vurderes opp mot virksomhetens kriterier for å akseptere risiko. Risikoen må håndteres dersom risikoen ikke anses som akseptabel.

Eksempel - Risikovurdering i anskaffelser

En oppdragsgiver skal anskaffe et IT-system som skal behandle og lagre informasjon i en skyløsning. Risikovurderingen identifiserer blant annet at følgende hendelse kan oppstå: *Uvedkommende kan få tilgang til informasjonen under overføringen mellom virksomheten og skytjenesten.* Hendelsen kan føre til følgende informasjonssikkerhetsbrudd: *Informasjonen kan komme på avveie.*

Deretter analyseres det hvor store disse konsekvensene er for virksomheten, før man vurderer sannsynligheten for at disse konsekvensene inntreffer som følge av en slik hendelse. Man har da funnet risikonivået (konsekvens og tilhørende sannsynlighet). Dette gjør det mulig å evaluere risikoen og prioritere hvilke risikoer som er akseptable og hvilke som må håndteres.

Risikovurderingen brukes til å finne ut hvilke krav som skal stilles i anskaffelsen. I dette tilfellet kan det stilles krav til å sikre kommunikasjonen mellom virksomheten og skytjenesten. Det kan også stilles krav til kryptering av informasjonen.

Resultatet av risikovurderingen kan presenteres i et overordnet risikonotat, som oppsummerer sentrale deler av vurderingen. Notatet kan brukes som et beslutningsgrunnlag for den videre håndteringen av risikoen. Vurderingen vil dermed være styrende for hvilke sikkerhetsrisikoer som skal reduseres eller imøtegås ved utformingen av kravene i anskaffelsen.

Dersom risikovurderingen viser at det er en sikkerhetsrisiko ved anskaffelsen som krever håndtering, må oppdragsgiver vurdere hvordan risikoen best kan ivaretas i anskaffelsen, hvilke krav som skal stilles, hvordan de skal utformes mv. Nærmere om adgangen til å stille krav til sikkerhet i anskaffelsesregelverket følger av kapittel 5. Oppdragsgiverne må i tillegg alltid følge kravene som lovgivningen stiller til sikkerhet, det være seg enten sikkerhetsloven med tilhørende forskrifter, personvernlovgivningen

eller annen lovgivning for øvrig. I en del tilfeller vil det være naturlig å ta utgangspunkt i forhåndsdefinerte standardkrav for ivaretakelse av sikkerhet ved den aktuelle typen anskaffelser. I så fall er det viktig at oppdragsgiverne tar selvstendig stilling til om kravene er relevante, og om det er krav som bør tas ut, eller om det er andre krav som bør legges til. Ved IKT-anskaffelser for statlige oppdragsgivere vil det for eksempel være relevant å se hen til kravene i Statens standardavtaler, nærmere omtalt i punkt 5.5.

Difi har utarbeidet en veiledning til gjennomføringen av risikovurderinger. Difis veiledning beskriver nærmere hvordan oppdragsgivere rent praktisk kan arbeide med risikovurderinger og hvordan disse kan resultere i konkrete krav i anskaffelsene.

Difis arbeid med veiledning om sikkerhet og risikovurderinger i IKT-anskaffelser

Difi har utarbeidet veiledning om informasjonssikkerhet, internkontroll og vern av personopplysninger i IKT-anskaffelser. Denne veiledningen inkluderer også gode råd til vurderinger av sikkerhet ved anskaffelser av skytjenester.

Difi har i tillegg etablert en arbeidsgruppe med blant annet NAV, Skatteetaten, NSM, Norsk helsenett og Direktoratet for eHelse. Arbeidsgruppen skal blant annet utarbeide spørsmål og eksempler på krav til informasjonssikkerhet i IKT-anskaffelser. Nedenfor følger lenker til Difis veiledning.

Veiledning til risikovurdering ved IKT-anskaffelser

Veiledning om internkontroll og informasjonssikkerhet

Eksempler på krav til informasjonssikkerhet – IKT-anskaffelser

Samleside for Difis veiledning om informasjonssikkerhet

Annen veiledning om IKT-sikkerhet og tjenesteutsetting

Utenfor sikkerhetslovens virkeområde er det utarbeidet generelle anbefalinger særskilt knyttet til IKT-sikkerhet. Anbefalingene er særlig knyttet til tjenesteutsetting og hva oppdragsgivere bør ha tenkt igjennom før valget om tjenesteutsetting tas. NSM har publisert følgende temarapporter som tar for seg utfordringer knyttet til tjenesteutsetting:

Sikkerhetsfaglige anbefalinger ved tjenesteutsetting og

Anbefalinger om landvurderinger ved tjenesteutsetting

Begge rapportene bygger på NSMs grunnprinsipper for IKT-sikkerhet.

4 Unntak fra anskaffelsesregelverket på sikkerhetsområdet

4.1 Innledning

Selv om en anskaffelse i utgangspunktet omfattes av anskaffelsesregelverket, kan den i visse tilfeller likevel unntas etter nærmere bestemmelser. Der unntaksbestemmelsene kommer til anvendelse, gjelder ikke anskaffelsesregelverket, og det vil ikke legge føringer på oppdragsgivernes valg av hvilke leverandører de vil inngå kontrakt med og på hvilke vilkår. I det følgende gjennomgås de mest sentrale unntaksbestemmelsene på sikkerhetsområdet.[35]

4.2 EØS-avtalen artikkel 123

Anskaffelsesregelverket kommer ikke til anvendelse på anskaffelser som kan unntas etter EØS-avtalen artikkel 123. Dette gjelder både anskaffelsesloven og de ulike forskriftene til denne.[36] Forsvarsdepartementet har gitt nærmere veiledning om unntaket i EØS-avtalen artikkel 123 i veilederen til FOSA, kapittel 7.2.

EØS-avtalen artikkel 123

Bestemmelsene i denne avtale skal ikke hindre en avtalepart i å treffe tiltak:

a) som den anser nødvendig for å hindre spredning av opplysninger som er i strid med dens vesentlige sikkerhetsinteresser;

b) som angår produksjon av eller handel med våpen, ammunisjon og krigsmateriell eller andre varer som er uunnværlige for forsvarsformål, eller forskning, utvikling eller produksjon som er uunnværlig for forsvarsformål, såfremt disse tiltak ikke endrer konkurransevilkårene for varer som ikke er bestemt for direkte militære formål;

[35] I veilederen til FOSA kapittel 7 er det gitt en mer utfyllende omtale av unntakene fra FOSAs virkeområde.

[36] Se anskaffelsesloven § 2 andre ledd, FOSA § 1-3(2) bokstav a, anskaffelsesforskriften § 2-2 første ledd bokstav b, forsyningsforskriften § 2-2 første ledd bokstav b og konsesjonskontrakforskriften § 2-8 bokstav a.

c) som den anser vesentlig for sin sikkerhet i tilfelle av alvorlig indre uro som truer den offentlige orden, i krigstid eller ved alvorlig internasjonal spenning som innebærer en fare for krig, eller for å oppfylle forpliktelser den har påtatt seg med sikte på å opprettholde fred og internasjonal sikkerhet.

Bestemmelsen har tre ulike unntak. Bokstav b retter seg mot militære forhold og utgjør dermed et såkalt «forvarsspesifikt» unntak. For oppdragsgivere utenfor forsvarssektoren er bokstav a og c de aktuelle unntakene. Bokstav a (informasjonssikkerhet) og bokstav c (forsyningssikkerhet) omfatter unntak for anskaffelser til blant annet kritisk infrastruktur som er av vesentlig sikkerhetsinteresse og øvrige sikkerhetsanskaffelser som gjennomføres i både militær og sivil sektor.

Det er opp til norske myndigheter å definere egne sikkerhetsinteresser og vurdere hvilke tiltak som er nødvendige for å beskytte disse. Terskelen for å bruke bestemmelsen er imidlertid høy, slik at ikke enhver sikkerhetsinteresse kan begrunne unntak fra anskaffelsesregelverket. Tiltakene må også underlegges en proporsjonalitetsvurdering, jf. det grunnleggende prinsippet i EØS-retten. Oppdragsgiver må derfor vurdere om sikkerhetsinteressene som eventuelt kan begrunne unntak kan ivaretas på en annen måte, for eksempel ved å stille krav til sikkerhet innenfor rammen av en anskaffelsesprosess i henhold til anskaffelsesregelverket. Hvis mindre inngripende tiltak enn å unnta anskaffelsen etter artikkel 123 er tilgjengelige, plikter oppdragsgiverne å benytte disse.

4.3 Unntak fra anskaffelsesforskriften for anskaffelser som gjelder sikkerhetsmessige forhold eller som er erklært hemmelige

Foruten anskaffelser som kan unntas etter artikkel 123, gir anskaffelsesforskriften § 2-2 adgang til å unnta anskaffelser som gjelder sikkerhetsmessige forhold eller som er erklært hemmelige, eller bare kan utføres under særlige sikkerhetstiltak.[37] Dersom vilkårene i bestemmelsen er oppfylt, kan oppdragsgiverne gjøre unntak fra både loven og forskriften.

[37] Tilsvarende unntak er gitt i forsyningsforskriften § 2-2, og et lignende unntak er gitt i konsesjonskontraktforskriften § 2-7.

Som det fremgår av kapittel 5, er det mange måter oppdragsgiverne kan ivareta sikkerhet på ved gjennomføringen av anskaffelsen. Det er verdt å merke seg at mange anskaffelser på sikkerhetsområdet omfattes av FOSA og ikke av anskaffelsesforskriften. Anvendelsesområdet for unntaksbestemmelsen i § 2-2 er i praksis snevert. Unntakene i § 2-2 skal, i likhet med de øvrige unntakene fra anskaffelsesregelverket, tolkes strengt, og det er oppdragsgiverne som må bevise at vilkårene er oppfylt.[38]

Anskaffelsesforskriften § 2-2 første ledd bokstav b inneholder et unntak for anskaffelser som er "*erklært hemmelige eller bare kan utføres under særlige sikkerhetstiltak i henhold til lov, forskrift eller forvaltningsvedtak, og de aktuelle vesentlige interessene ikke kan sikres gjennom mindre inngripende tiltak*". Denne delen av bestemmelsen inneholder to unntak: 1) der anskaffelsen er *erklært hemmelig*, og 2) der anskaffelsen *bare kan utføres under særlige sikkerhetstiltak*. Det første unntaket i bestemmelsen, anskaffelser som er *erklært hemmelige,* viser til anskaffelser som er sikkerhetsgradert på nivå "hemmelig" eller over etter nasjonal lovgivning eller et forvaltningsvedtak. Denne graderingen benyttes i sikkerhetsloven § 5-3 bokstav a (STRENGT HEMMELIG) og bokstav b (HEMMELIG), og anskaffelser med slik gradering vil normalt kunne unntas fra anskaffelsesforskriften.[39] [40] Det er selve eksistensen av anskaffelsen og gjennomføringen av kontrakten, som må ha graderingen "hemmelig".[41]

Dette unntaket vil derfor ha et svært snevert anvendelsesområde i praksis. Anskaffelser som er erklært hemmelige etter sikkerhetsloven vil i de aller fleste tilfeller falle innenfor FOSAs anvendelsesområde, og ikke anskaffelsesforskriften. Det vil være få tilfeller der

---

[38] Se f.eks. sak C-187/16 (*Kommisjonen mot Østerrike*), premiss 77 og 78.

[39] Derimot omfatter ikke dette unntaket anskaffelser som har en lavere sikkerhetsgradering enn hemmelig, for eksempel anskaffelser som etter sikkerhetsloven § 5-3 har en sikkerhetsgradering KONFIDENSIELT eller BEGRENSET.

[40] Det kan i prinsippet tenkes at også andre interesser enn nasjonale sikkerhetsinteresser kan berettige gradering som "hemmelig". I litteraturen er det vist til at unntaket muligens kan anvendes, for eksempel, for å beskytte personvernopplysninger eller statlige forretningshemmeligheter – se Arrowsmith Vol 1, side 487.

[41] Se direktiv 2014/24/EU artikkel 15 nr. 3 der det fremgår følgende: *Where the procurement and performance of the public contract or design contest are declared to be secret"* (vår understerking). Se også Arrowsmith Vol 2 , side 200.

en anskaffelse, som faller utenfor forsvars- og sikkerhetsområdet, i sin helhet erklæres hemmelig.

Den andre unntaket i bestemmelsen, anskaffelser som *bare kan utføres under særlige sikkerhetstiltak*, omfatter blant annet sikkerhetstiltak i henhold til sikkerhetsloven. Unntaket kan blant annet omfatte tilfeller der anskaffelsens eksistens og gjennomføringen av kontrakten ikke er gradert som "hemmelig". For eksempel kan unntaket omfatte tilfeller der anskaffelsen er gitt et lavere graderingsnivå, eller der kun deler av anskaffelsen, for eksempel kravspesifikasjonen til utstyret som anskaffes, eller informasjonen som må håndteres av leverandøren i forbindelse med anskaffelsen eller kontraktsgjennomføringen, blir gitt en gradering.[42] Særlige sikkerhetstiltak må i alle tilfeller være hjemlet i lov, forskrift eller forvaltningsvedtak. Også dette unntaket har et snevert anvendelsesområde i praksis, blant annet fordi de fleste anskaffelser som fordrer særlige sikkerhetstiltak faller innenfor FOSAs anvendelsesområde, og ikke anskaffelsesforskriften.

Felles for begge unntakene i anskaffelsesforskriften § 2-2 første ledd bokstav b, er at de bare kommer til anvendelse dersom *de aktuelle vesentlige interessene ikke kan sikres gjennom mindre inngripende tiltak.* EU-domstolen har for denne delen av unntaket anvendt en form for forholdsmessighetsvurdering, og praksis viser at det skal mye til for at unntaket kommer til anvendelse. Forholdsmessighetsvurderingen omtales nærmere under punkt 4.3.1.

Anskaffelsesforskriften § 2-2 andre ledd hjemler unntak fra anskaffelsesregelverket dersom anvendelsen av regelverket vil forhindre oppdragsgiveren i å ivareta vesentlige sikkerhetsinteresser. Dette unntaket synes å omfatte de samme typetilfellene som er omfattet av unntakene i § 2-2 første ledd bokstav b.[43] [44] I motsetning til tilfellene i § 2-2

---

[42] Arrowsmith Vol 2. side 200-201.

[43] EU-domstolen foretok i sak C-187/16 en samlet vurdering av tilsvarende unntak i det tidligere direktiv 2004/18/EC.

[44] Under henvisning til direktiv 2014/24/EU artikkel 15 nr. 2 som angir at "*This Directive shall not apply to public contracts […] to the extent that the protection of the essential security interests of a Member State cannot be guaranteed by less intrusive measures*" (vår understerking), fremhever Arrowsmith at ordlyden kan indikere at unntaket bare kan benyttes til å unnta anskaffelsen fra direktivets prosedyreregler i den grad det er nødvendig for å ivareta de vesentlige sikkerhetsinteressene, og at

første ledd bokstav b, er det for bestemmelsen i andre ledd ikke et krav om at unntaket er hjemlet i lov, forskrift eller forvaltningsvedtak.

Som for første ledd, kommer heller ikke unntaket i § 2-2 andre ledd til anvendelse *dersom oppdragsgiveren kan ivareta de vesentlige sikkerhetsinteressene gjennom mindre inngripende tiltak, for eksempel ved å pålegge leverandørene taushetsplikt.* Også dette gir anvisning på en forholdsmessighetsvurdering.

4.3.1 Nærmere om forholdsmessighetsvurderingen

Unntak på bakgrunn av sikkerhetsmessige forhold må som nevnt være forholdsmessig.[45] Unntakene kan bare anvendes dersom de aktuelle interessene ikke kan sikres gjennom mindre inngripende tiltak. Anskaffelsesforskriften nevner for eksempel at sikkerhetsinteressene kan ivaretas ved å pålegge leverandørene taushetsplikt.

EU-domstolen har ved flere tilfeller uttalt seg om forholdsmessighetsvurderingen ved bruk av disse unntakene, se eksempelvis sak C-187/16 (*Kommisjonen mot Østerrike*) som omtales nærmere nedenfor.[46] Praksisen viser at oppdragsgiverne i utgangspunktet står nokså fritt til å selv definere hvilke vesentlige sikkerhetsinteresser de anser som legitime å ivareta, men at de må angi gode og utfyllende begrunnelser for hvorfor interessene ikke kan ivaretas gjennom andre tiltak, innenfor rammene av en anskaffelsesprosess i henhold til forskriften. Praksis viser også at domstolen foretar nøye vurderinger av oppdragsgivernes begrunnelser, og at det skal nokså mye til for at sikkerhetsunntakene

---

bestemmelsen ikke gir hjemmel for å gjøre unntak alle direktivets prosedyreregler. Dette er i så fall en forskjell fra unntakene i § 2-2 første ledd bokstav b. Se Arrowsmith Vol 1. side 490-491.

[45] Det vil si unntaket i § 2-2 første ledd bokstav b og § 2-2 andre ledd.

[46] Dommen er avsagt etter tidligere anskaffelsesdirektiv, direktiv 2004/18/EF. Avgjørelsen gir likevel god veiledning om forholdsmessighetsvurderingen i anskaffelsesforsrkfiten § 2-2 første ledd bokstav b og andre ledd, som bygger på tilsvarende unntak i det nye anskaffelsesdirektivet 2014/24/EU. Andre avgjørelser som bygger på lignende unntak i tidligere anskaffelsesdirektiv kan også gi veiledning om forholdsmessighetsvurderingen, slik som sakene C-324/93 *(Evans Medical)*, C-252/01 (*Belgian Aerial Photography)*, og C-157/06 (*Augusta Helicopters)*. Disse avgjørelsene er gitt en nærmere omtale i Arrowsmith Vol. 2, se blant annet 201-202.

kommer til anvendelse, ettersom høye krav til sikkerhet ofte kan ivaretas på en tilstrekkelig måte gjennom en anskaffelsesprosess.

På generelt grunnlag vil unntak fra anskaffelsesforskriften kunne anses forholdsmessig dersom oppdragsgiveren har et legitimt ønske om ikke å avdekke sikkerhetsrelatert informasjon til leverandører fra andre land.[47] Anskaffelser vil også kunne unntas i den utstrekning som er nødvendig for hindre at en medlemsstat blir avhengig av leveranser fra et tredjeland eller leverandører som er hjemmehørende i tredjeland.[48] Dette er i praksis en høy terskel.

Ut fra disse betraktningene kan vurderingen bli noe forskjellig alt etter om det er snakk om produksjon av varer og tjenester i en fremmed stat, eller om en utenlandsk leverandør skal utføre leveransen i Norge. Det antas at oppdragsgiverne vil ha en større grad av kontroll og større mulighet til å kreve betryggende sikkerhetstiltak dersom arbeidet med leveransen utføres i Norge.

Rettsavgjørelse

C-187/16 (*Kommisjonen mot Østerrike*), gjaldt en sak der en østerriksk oppdragsgiver kjøpte tjenester for trykking av pass og id-papirer direkte fra den østerrikske leverandøren ÖS under henvisning til unntaket for sikkerhetsmessige forhold i de tidligere anskaffelsesdirektivene, som tilsvarer dagens sikkerhetsunntak. Kommisjonen mente vilkårene for unntak ikke var oppfylt, og brakte saken inn for EU-domstolen. EU-domstolen anerkjente at det var vesentlige sikkerhetsinteresser som var nødvendige å ivareta i forbindelse med anskaffelsen, men mente Østerrike ikke hadde godtgjort at disse interessene ikke kunne ivaretas innenfor rammen av en anskaffelsesprosedyre i henhold til direktivet.

For det første avslo domstolen Østerrikes argument om at anskaffelsen samlet sett måtte tildeles én leverandør – å tildele kontrakten til én leverandør kunne gjøres etter en anskaffelsesprosedyre.

For det andre avslo domstolen et argument om at det var nødvendig å tildele kontrakten til ÖS, fordi det var nødvendig å tildele kontrakten til en leverandør i Østerrike for å sikre et effektiv administrativt tilsyn med at kravene til sikkerhet,

[47] Generaladvokatens uttalelse i sak C-187/16, premiss 70.

[48] Generaladvokatens uttalelse i sak C-187/16, premiss 70.

herunder kravene til konfidensialitet, ble etterlevd. Domstolen mente det ikke var gitt begrunnelse for hvorfor slikt tilsyn ikke kunne være like effektivt overfor andre leverandører etablert i Østerrike. Videre viste domstolen til at det ikke var gitt begrunnelse for hvorfor det ikke var tilstrekkelig å innta kontraktsvilkår om konfidensialitet og andre sikkerhetskrav, herunder innta krav om sikkerhetskontroll, besøk og inspeksjoner i lokalene til leverandørene, uavhengig av om leverandørene befant seg i Østerrike eller i et annet medlemsland.

For det tredje kom domstolen til at det ikke var godt nok begrunnet at hensynet til forsyningssikkerhet ikke kunne ivaretas gjennom en anskaffelsesprosedyre.

For det fjerde avslo domstolen et argument om at leverandørens pålitelighet ikke kunne sikres gjennom en anskaffelsesprosedyre.

5 Hvordan stille krav til ivaretakelse av sikkerhet etter anskaffelsesforskriften mv.

5.1 Innledning

Anskaffelsesregelverket åpner for at oppdragsgiverne kan stille krav til ivaretakelse av sikkerhet på mange måter i anskaffelsene sine. I dette kapittelet vil vi først og fremst se på hvordan oppdragsgiverne kan ivareta hensynet til sikkerhet i anskaffelser som ikke omfattes av sikkerhetsloven eller FOSA.[49]

Anskaffelsesforskriften, forsyningsforskriften og konsesjonskontraktforskriften gir blant annet adgang til å stille krav til *fysisk sikkerhet*, gjennom for eksempel adgangskontroll eller krav til byggsikkerhet. Forskriftene gir også adgang til å stille krav til *informasjonssikkerhet*, gjennom for eksempel krav til konfidensialitet og informasjonshåndtering. Dette omfatter for eksempel krav til sikkerhet i IKT-anskaffelser. Kravene kan stilles i flere faser av anskaffelsene, både i kravspesifikasjonen, kvalifikasjonskravene, tildelingskriteriene eller i kontraktsvilkårene.

Sikkerhetskravene skal ivareta og imøtegå de risikomomentene som er identifisert i risikovurderingen, i forkant av anskaffelsen.[50] Kravene til ivaretakelse av sikkerhet bør ikke gå lengre enn hva som er nødvendig for å imøtegå sikkerhetsrisikoen ved en anskaffelse, jf. forholdsmessighetsprinsippet. I anskaffelser som ikke er underlagt sikkerhetsloven eller FOSA, må krav til ivaretakelse av sikkerhet veies opp mot andre hensyn som oppdragsgiver skal ivareta.[51] Dersom det stilles strenge sikkerhetskrav, kan dette begrense antallet tilbydere som kan konkurrere om oppdraget. Strenge

---

[49] Se veiledere til sikkerhetsloven og FOSA for nærmere informasjon om hvordan man ivaretar hensynet til sikkerhet etter dette regelverket. FOSA inneholder for eksempel flere særskilte hjemler for ivaretakelse av sikkerhet. Mange av betraktningene i dette kapittelet kan likevel være relevant også for anskaffelser etter FOSA.

[50] Gjennomføringen av risikovurderinger er omtalt i kapittel 3, der det blant annet vises til Difis veiledning om temaet.

[51] I tillegg må oppdragsgiver selvfølgelig ivareta eventuelle andre lovkrav i andre regelverk som stiller krav knyttet til sikkerhet.

sikkerhetskrav kan særlig påvirke små og mellomstore bedrifters muligheter for å delta i konkurransen.

Mulighetene til å stille krav til ivaretakelse av sikkerhet i anskaffelsene vil også ha betydning for adgangen til å bruke unntaket som gjelder sikkerhetsmessige forhold.[52] Det følger av EU-domstolens praksis at det bare er i tilfeller hvor den aktuelle sikkerhetsinteressen ikke kan ivaretas på en annen måte, at det er mulig å gjøre unntak fra regelverket.[53] Det betyr at oppdragsgiverne må vurdere om krav som stilles i anskaffelsen er tilstrekkelig for å ivareta sikkerhetsinteressene, før det eventuelt gjøres unntak. Adgangen til å gjøre unntak for anskaffelser som gjelder sikkerhetsmessige forhold er nærmere beskrevet i kapittel 4.

I dette kapittelet vil vi se nærmere på hvordan krav til ivaretakelse av sikkerhet kan stilles i de forskjellige fasene av anskaffelsesprosessen. Kapittelet inneholder også eksempler på forskjellige måter å ivareta sikkerhet på. Gjennomgangen er ikke ment som en uttømmende liste, og oppdragsgivere må vurdere konkret hvilke krav til ivaretakelse av sikkerhet som er nødvendig og forholdsmessig i den aktuelle anskaffelsen.

Anskaffelsesregelverket omfatter flere forskrifter. I dette kapittelet vises det til bestemmelsene i anskaffelsesforskriften, men mulighetene som beskrives i dette kapittelet vil i stor grad også være relevant for anskaffelser som følger forsyningsforskriften og konsesjonskontraktforskriften. Som vist i punkt 2.1 kan enkelte anskaffelser følge sikkerhetsloven og anskaffelsesforskriften, forsyningsforskriften eller konsesjonskontraktsforskriften.

Nærings- og fiskeridepartementet har gitt nærmere veiledning til anskaffelsesforskriften på departementets nettsider. Veilederen til anskaffelsesforskriften gir blant annet veiledning til bestemmelsene om kravspesifikasjoner, kvalifikasjonskrav og tildelingskriterier.

Konfidensialitet og avvisning

EU-domstolen har uttalt at oppdragsgiverne har mulighet til å innta, som et krav i konkurransen, at den vinnende leverandøren må overholde forpliktelser om generell

[52] Se kapittel 4 om unntak fra anskaffelsesregelverket på sikkerhetsområdet.

[53] Sak EU-domstolens sak C-187/16. Saken er nærmere beskrevet over i punkt 4.3.1.

konfidensialitet, samt at manglende garantier for overholdelse av et slik krav, da særlig på grunn av lovbestemmelser i hjemlandet til leverandøren, vil føre til avvisning.[54]

Uttalelsen må ses i lys av betydningen av konfidensialitet mellom oppdragsgiveren og dens leverandør. Oppdragsgiveren må kunne stole på at leverandøren ikke sprer eller videreformidler taushetsbelagt informasjon.[55] Dette er helt sentralt for å ivareta konfidensialiteten ved utføringen av oppdraget. Leverandører fra enkelte land er samtidig underlagt lovbestemmelser som pålegger dem et potensielt utstrakt samarbeid med statlige myndigheter, for eksempel sikkerhetsmyndighetene i hjemlandet. Slike bestemmelser kan også omfatte videreformidling av taushetsbelagt informasjon. Oppdragsgivere som inngår kontrakter med leverandører som er underlagt jurisdiksjonen til denne typen land, risikerer dermed at leverandøren blir pålagt å videreformidle informasjon til myndighetene i hjemlandet, også informasjon som er å anse som konfidensiell i henhold til kontrakten.

Oppdragsgiverne må alltid vurdere forholdsmessigheten av et slikt konfidensialitetskrav. Det må blant annet tas stilling til hvor sensitive de aktuelle opplysningene er, hvordan kravet vil påvirke konkurransen og hvor stor den faktiske risikoen er for at hjemmelen i lovbestemmelsen tas i bruk.[56]

Anskaffelsesforskriften § 7-4 gir oppdragsgiverne mulighet til å stille krav til leverandørene om å beskytte informasjon av fortrolig karakter som gjøres tilgjengelig for dem i forbindelse med en anskaffelse.

5.2 Sikkerhet i kravspesifikasjonene

Kravspesifikasjonene angir kravene som stilles til egenskapene til det som skal anskaffes.[57] Kravspesifikasjonene kan utformes enten som ytelses- eller

---

[54] Se EU-domstolen avgjørelse i sak C-187/16, avsnitt 92 og 93.

[55] Dette kan også omfatte informasjon som ikke er gradert som konfidensielt etter sikkerhetsloven § 5-3, men som er å anse som taushetsbelagt eller sensitiv på annet grunnlag, for eksempel opplysninger som er omfattet av annen lovgivning, beskyttelsesinstruksen eller forretningshemmeligheter.

[56] Se EU-domstolen avgjørelse i sak C-187/16, avsnitt 92 og 93.

[57] Jf. anskaffelsesforskriften § 15-1 første ledd.

funksjonsbeskrivelser, ved bruk av tekniske spesifikasjoner eller ved en kombinasjon av disse.

Oppdragsgiverne har stor grad av skjønnsfrihet til å bestemme hva som skal anskaffes, noe som reflekteres i forskriftsbestemmelsen om kravspesifikasjoner. Denne skjønnsfriheten gjelder også muligheten til å stille krav til ivaretakelse av sikkerhet. Sikkerhetskravene kan relatere seg til alle sider av og trinn i livssyklusen til leveransen, og det er mulig å stille krav til sikkerhet som omfatter delkomponenter, støttefunksjoner og andre tekniske aspekter.

Kravspesifikasjonen kan inneholde en kombinasjon av absolutte krav og såkalte *bør-krav*. De absolutte kravene angir minimumsnivået av sikkerhetskrav som leveransen må ivareta for at tilbudet ikke skal bli avvist. Bør-kravene kan omfatte håndtering av sikkerhetsrisiko, ut over det oppdragsgiveren anser som et minimumsnivå. Bør-kravene kan for eksempel stilles i et spørsmål-og-svar-format, hvor oppdragsgiveren ber leverandørene redegjøre for hvordan de vil håndtere ulike spørsmål knyttet til sikkerhet. Svarene kan gi oppdragsgiveren en forståelse av hvordan leverandøren vil ivareta sikkerheten. Besvarelser knyttet til bør-kravene kan for eksempel brukes ved evalueringen av tilbudet, som grunnlag for vurderingen av tilbudets kvalitet.

Bruk av funksjonskrav for ivaretakelse av sikkerhet

Oppdragsgiverne kan vurdere om krav til sikkerhet kan ivaretas gjennom funksjonskrav. Funksjons- og ytelseskrav retter seg mot leveransens resultater og effekter istedenfor å stille krav til konkret løsning. Når det gjelder krav til ivaretakelse av sikkerhet, kan oppdragsgiverne for eksempel stille som et funksjonskrav at løsningen skal sikre lagret informasjon istedenfor at det stilles spesifikke krav til hvordan informasjonen skal sikres. Anskaffelsen vil da åpne opp for tilbud som på ulike måter møter behovet for å sikre lagret informasjon.

Videre kan oppdragsgiverne stille krav om at leverandørene skal fremlegge en testrapport fra et samsvarsvurderingsorgan.[58] Et samsvarsvurderingsorgan er et akkreditert organ som blant annet driver med kalibrering, testing, sertifisering og inspeksjon. I Norge er Norsk Akkreditering et slikt samsvarsvurderingsorgan. På denne

[58] Jf. anskaffelsesforskriften § 15-4.

måten kan oppdragsgiverne få en uavhengig tredjepartsvurdering som bekrefter at leveransen oppfyller kravspesifikasjonen, tildelingskriteriene eller kontraktsvilkårene.

Kravene i kravspesifikasjonen må ha tilknytning til leveransen og stå i forhold til anskaffelsens formål og verdi. Tilknytningskravet innebærer at oppdragsgiverne ikke kan knytte krav til forhold som ligger utenfor anskaffelsen. Krav om fysisk sikkerhet, for eksempel gjennom adgangskontroll ved produksjonsstedet, vil derfor normalt anses å ha den nødvendige tilknytningen til leveransen. Motsetningsvis kan et krav om fysisk sikkerhet på leverandørens andre produksjonssteder være problematisk.

5.3 Sikkerhet i kvalifikasjonskravene

Oppdragsgiverne kan stille krav til leverandørenes kvalifikasjoner gjennom bruk av kvalifikasjonskrav. Særlig relevant i et sikkerhetsperspektiv er kravene til leverandørenes tekniske og faglige kvalifikasjoner. Anskaffelsesforskriften del III inneholder en uttømmende regulering av hvilke krav til dokumentasjon oppdragsgiverne kan be om som bekreftelse på leverandørenes tekniske og faglige kvalifikasjoner. Leverandører som ikke oppfyller kvalifikasjonskravene skal avvises.

Oppdragsgiverne kan blant annet stille krav til at leverandørene skal kunne dokumentere erfaring fra liknende eller tilsvarende oppdrag.[59] På denne måten kan oppdragsgiverne sikre at leverandørene har erfaring med ivaretakelse av sikkerhet i det omfang og den utstrekning som er nødvendig eller ønskelig for utførelsen av leveransen. Krav til erfaring fra tidligere oppdrag kan samtidig utelukke små og mellomstore bedrifter eller bedrifter i oppstartsfasen fra å delta i konkurransen. Som et alternativt dokumentasjonskrav, kan oppdragsgiverne derfor innta at leverandørene kan dokumentere erfaringen ved å vise til erfaring hos personell i bedriften, uavhengig av om erfaringen er opparbeidet mens personellet arbeidet for en annen leverandør.

Erfaring fra tilsvarende oppdrag er relevant der erfaringen kan ha betydning for utførelsen av oppdraget. Det kan for eksempel være relevant ved tjenester som omfatter feilretting eller håndtering av dataangrep. Hvordan og hvor raskt en feil rettes, kan ha stor betydning for bruken av tjenesten. Hvordan et eventuelt dataangrep håndteres, kan ha stor betydning for mulighetene til å begrense skade. Erfaring fra tidligere oppdrag kan på den måten vise at leverandøren er kompetent til å håndtere den aktuelle sikkerhetsrisikoen. Feilretting og håndtering av dataangrep er viktige

[59] Jf. anskaffelsesforskriften § 16-6 første ledd bokstav a) og b).

spørsmål, som også kan gjøres til et tema i en eventuell spørsmål-og-svar-runde, og det kan tillegges vekt ved evalueringen av tilbudene.

Gjennom kvalifikasjonskravene kan oppdragsgiverne stille krav knyttet til teknisk personell eller tekniske enheter, og da særlig de som er ansvarlig for kvalitetskontrollen.[60] Tilfredsstillende kvalitetskontroll kan for eksempel ha betydning for etterlevelsen av sikkerhetskravene.

Oppdragsgiverne har også mulighet til, som en del av kvalifikasjonskravene, å kreve dokumentasjon på oppfyllelse av visse kvalitetssikringsstandarder.[61] Som dokumentasjon på styringssystem i informasjonssikkerhet, kan oppdragsgiverne for eksempel kreve fremlagt attest for oppfyllelse av ISO 27001 eller tilsvarende. Attest for oppfyllelse av kvalitetssikringsstandarder kan være ressurskrevende for levererandørene å innhente. Oppdragsgiverne må derfor vurdere nødvendigheten av et slikt krav i lys av hvordan dette kan påvirke konkurransen.

I tillegg kan oppdragsgiverne stille visse krav til testing og kontroll i kvalifikasjonskravene. Disse mulighetene er omtalt i punkt 5.4.1 under.

5.4 Sikkerhet i tildelingskriteriene

Tildelingskriteriene er kriteriene som brukes til å foreta en rangering av tilbudene. I anskaffelser der oppdragsgiverne skal velge tilbud på grunnlag av beste forhold mellom pris og kvalitet, kan ivaretakelse av sikkerhet for eksempel brukes i forbindelse med vurderingen av tilbudets kvalitet.

Tildelingskriteriene egner seg ikke til å stille krav som er helt nødvendig for å ivareta sikkerheten til virksomheten eller de offentlige tjenestene. Eventuelle kriterier knyttet til sikkerhet bør derfor heller benyttes for å oppnå en merverdi ut over minstekravene i anskaffelsen. Kriteriene kan for eksempel omfatte forhold som kompetanse hos tilbudt nøkkelpersonell, kortere responstid eller kortere nedetid enn angitt i kravspesifikasjonen, samt oppfyllelse av andre bør-krav i kravspesifikasjonen.

Tildelingskriteriene skal ha tilknytning til leveransen, noe som betyr at kriteriene må relatere seg til det som skal leveres under kontrakten. Kriteriene kan heller ikke være så

[60] Jf. anskaffelsesforskriften § 16-6 første ledd bokstav c).

[61] Jf. anskaffelsesforskriften § 16-7.

skjønnspregede at de gir oppdragsgiveren en ubegrenset valgfrihet ved vurderingen av tilbudene.[62]

Vektlegging av sikkerhet ved vurderingen av tilbudets kvalitet

I en IKT-anskaffelse har oppdragsgiveren stilt som et bør-krav at sikkerheten bør ivaretas ved bruk av anerkjente, relevante sikkerhetsstandarder med tilknytning til tjenesten. Leverandørene blir bedt om å beskrive hvilke standarder og sertifiseringer de overholder, som eksempelvis ISO 27002, ISO 27017, ISO 27018, ISO 22313, eller tilsvarende.

Oppdragsgiver stiller med dette ikke et absolutt krav om sertifisering, men kan i evalueringen premiere dem som følger relevante standarder og som da gir en kvalitativ merverdi ved at det skaper sikkerhetsmessig trygghet for at leverandøren bruker bestepraksis og anerkjente metoder for produksjon og levering av tjenesten.

5.4.1 Testing av leveransen

Testing av leveransen er en god måte for oppdragsgiverne å skaffe seg kjennskap til de sikkerhetsmessige sidene ved leveransen. Testing kan være hensiktsmessig av flere grunner. Det kan være i oppdragsgiverens interesse i tilfeller der anskaffelsen åpner for eller legger opp til å ta i bruk ny teknologi, eller i anskaffelser hvor det ikke er mulig å kartlegge sikkerhetsprofilen til leveransen fullt ut på forhånd. Situasjonen kan også være den at oppdragsgiveren ønsker selv å undersøke de tilbudte løsningene, for på den måten å verifisere opplysninger gitt av leverandøren.

Oppdragsgiverne kan utføre testing eller utprøving av leveransen i forbindelse med tilbudsevalueringen. Testingen kan gjennomføres enten av oppdragsgiveren selv eller ved hjelp av en representant for oppdragsgiver. Oppdragsgiveren kan utføre testingen på den måte han finner hensiktsmessig. Testingen kan således være dyptgående og omfatte alle potensielle sikkerhetsrisikoer ved leveransen. Testingen må likevel gjennomføres i tråd med de grunnleggende prinsippene, herunder prinsippene om likebehandling, forutberegnelighet og etterprøvbarhet. I utgangspunktet skal testingen

[62] Begrensningene følger av anskaffelsesforskriften § 18-1 og forsyningsforskriftren 14-1. Det er gitt nærmere veiledning om hva som ligger i begrensningene i veiledningen til anskaffelsesforskriften på departementets hjemmeside.

utføres på samme måte for alle leverandørene, og dersom testingen er beskrevet i anskaffelsesdokumentene, skal testingen utføres på en måte som i all hovedsak tilsvarer denne beskrivelsen.[63]

Testing for programvarefeil i IKT-systemer

Kravene i anskaffelsen danner utgangspunktet for testingen av leveransen. Dersom risikoen i anskaffelsen anses som høy, bør det gjennomføres spesifikk sikkerhetstesting. Programvarefeil kan gjøre systemene mer mottakelig for angrep og kan føre til nedetid og kritisk stans i behandlingen av oppgaver. NSM har pekt på at de ser stadig flere målrettede nettverksoperasjoner mot både private og offentlige virksomheter.[64] Sårbare systemer og enkel tilgang til skadevare har ved flere tilfeller ført til at norske virksomheters informasjonssystemer har blitt kompromittert. Testing av leveransen kan gi oppdragsgiverne et mer realistisk bilde av risikoen for feil i programvaren, og det kan også si noe om hvor mottakelig systemet er for angrep utenfra. I anskaffelser med høy risiko kan det for eksempel gjennomføres en penetrasjonstest. Gjennomføring av tester er ofte tid- og ressurskrevende, og oppdragsgiver må i så fall sette av tid og ressurser til dette i planleggingen av anskaffelsen. Statens standardavtaler for IKT-anskaffelser inneholder detaljerte bestemmelser om testing av leveransen. Disse avtalene er nærmere beskrevet i boksen nedenfor.

Også kvalifikasjonskravene inneholder visse muligheter til å gjennomføre testing og kontroll. Ved anskaffelser av varer kan oppdragsgiverne etterspørre dokumentasjon i

[63] Utgangspunktet om testingen skal gjennomføres på samme måte gjelder likevel ikke ubetinget. Det må være en rimelig proporsjonalitet mellom det som skal oppnås med testingen og ulempen og kostnaden for leverandøren, jf. for eksempel KOFA-sak 2005/198. Oppdragsgiveren kan også unnlate å teste enkelte leverandører dersom de uansett ikke har mulighet til å nå opp i konkurransen. I tillegg kan oppdragsgiveren i enkelte tilfeller unnlate å teste produkter han allerede er kjent med, jf. for eksempel KOFA-sak 2006/90.

[64] Se Nasjonal Sikkerhetsmyndighet (NSM), *Risiko 2019 – Krafttak for et sikrere Norge*, s. 11.

form av vareprøver.[65] Tilgang til vareprøver gir oppdragsgiverne mulighet til å på egenhånd teste om varene leverandøren tilbyr oppfyller sikkerhetskravene som er stilt i anskaffelsen, som igjen vil kunne si noe om leverandørens tekniske og faglige kvalifikasjoner er oppfylt.

I tillegg kan oppdragsgiverne ved anskaffelser av varer og tjenester som er kompliserte, kontrollere leverandørens produksjonskapasitet eller tekniske kapasitet, samt også leverandørenes tilgjengelige kvalitetskontrolltiltak mv.[66] Kontrollen kan også omfatte de sikkerhetsmessige sidene ved leverandørenes kapasitet og kvalitetskontrolltiltak.

5.5 Sikkerhet i kontraktsvilkårene

Kontraktsvilkårene inneholder bestemmelser for gjennomføringen av kontrakten. Kontraktsfasen er i utgangspunktet ikke regulert av anskaffelsesregelverket, og bestemmelsen om kontraktsvilkår angir i korte trekk at oppdragsgiver kan fastsette kontraktsvilkår og at disse må ha tilknytning til leveransen og fremgå av anskaffelsesdokumentene.[67]

Bruk av Statens standardavtaler

Statens standardavtaler (SSA) er de mest brukte kontraktsmalene for IKT-anskaffelser i offentlig sektor og anbefalt standard i Referansekatalogen for IT-standarder. Avtalene har også stor utbredelse i privat sektor. I SSA-ene er det beskrevet et omfattende testregime med krav både til leverandørens og kundens testing før kunden aksepterer leveransen. Standardavtalene inneholder også egne kapitler med krav til informasjonssikkerhet generelt, og til personvern. SSA-ene forvaltes av Difi.[68]

Kontraktsvilkårene regulerer forholdet mellom oppdragsgiverne og leverandørene i løpet av kontraktsfasen. Oppdragsgiverne kan benytte seg av en rekke kontraktsvilkår knyttet til ivaretakelse av sikkerhet. Krav til sikkerhet kan for eksempel ivaretas gjennom krav til konfidensialitet, mulighet for revisjon og stedlig kontroll, samt sanksjoner ved

[65] Jf. anskaffelsesforskriften § 16-6 andre ledd.

[66] Jf. anskaffelsesforskriften § 16-6 tredje ledd.

[67] Jf. anskaffelsesforskriften § 19-1.

[68] Se Referansekatalogen på Difis nettsider.

mislighold. Gjennom denne typen vilkår forpliktes leverandøren til å overholde sikkerhetskravene i kontrakten for øvrig, og oppdragsgiveren gis mulighet til etterprøve leverandørens opplysninger.

Som et ledd i en eventuell revisjon, kan oppdragsgiverne reservere seg muligheten til å gjennomføre tester av leveransen. På denne måten kan oppdragsgiverne få en bekreftelse på at ikke bare tilbudet er i tråd med sikkerhetskravene, men at også den faktiske leveransen overholder disse kravene.[69]

I anskaffelser hvor sikkerhetsaspektet anses å være av særlig betydning, kan oppdragsgiverne ha interesse av å begrense mulighetene for bruk av underleverandører for de delene av anskaffelsen som knytter seg til ivaretakelse av sikkerhet. Ved anskaffelser av varer som inkluderer montering- og installasjonsarbeid, tjenester og bygge- og anleggsarbeider, gir anskaffelsesforskriften og forsyningsforskriften oppdragsgiverne adgang til å stille krav om at bestemte kritiske oppgaver skal utføres av leverandøren selv. Denne adgangen er omtalt både i forbindelse med støtte fra andre virksomheter og i bestemmelsen om bruk av underleverandører.[70] Kritiske oppgaver må forstås som sentrale elementer ved leveransen, som i vesentlig grad bidrar til oppfyllelse av kontrakten. Oppgaven kan for eksempel forutsette stor grad av samarbeid mellom oppdragsgiveren og leverandøren over tid, eller det kan være at oppgaven er av en særlig konfidensiell karakter.[71]

I kontraktsvilkårene kan oppdragsgiverne også ta høyde for eventuelle endringer underveis i kontraktsforløpet. Oppdragsgiverne kan da for eksempel innta en opsjon som angir at leveransen skal oppdateres for å møte endringer i sikkerhetsrisikoen i løpet av kontraktsperioden.[72] Den konkrete utformingen av opsjonen må bero på en

---

[69] Slike tester eller revisjoner kan gjennomføres på flere forskjellige måter. Testing av leveransen kan gjøres på overtakelsestidspunktet, for eksempel i forbindelse med overtakelsen av leveransen, eller det kan gjennomføres kontroll i løpet av kontraktsperioden, for eksempel ved utførelsen av tjenester.

[70] Jf. anskaffelsesforskriften § 19-2 andre ledd og forsyningsforskriften § 19-2 andre ledd.

[71] Se departementets veileder til anskaffelsesforskriften, punkt 22.3 om støtte fra andre virksomheter.

[72] Jf. anskaffelsesforskriften §§ 16-10 sjette ledd og 19-1 andre ledd og forsyningsforskriften §§ 12-5 sjette ledd og 15-1 andre ledd.

vurdering av det aktuelle trusselbildet og mulighetene for å gjøre oppdateringer og endringer underveis i kontraktsforløpet.

Kontraktsvilkårene kan også omfatte en rett for oppdragsgiverne til å tre ut av avtalen dersom visse forhold foreligger. Endrede eierforhold hos leverandøren, for eksempel til eiere fra land Norge ikke har et sikkerhetsmessig samarbeid med, er et eksempel på et forhold som kan utløse en mulig rett til å tre ut av avtalen. En slik rett til uttreden bør kombineres med en plikt for leverandøren til å melde fra om eventuelle endringer i eierforholdene i løpet av kontraktsperioden. I kontaktsvilkårene kan oppdragsgivere også regulere hvordan en slik uttreden kan gjennomføres, for eksempel ved at oppdragsgiver får mulighet til å tilbakeføre data til eget system, eller overføre data til en annen leverandør på forsvarlig måte.

Utgitt av:
Nærings- og fiskeridepartementet og Forsvardepartementet