DET KONGELIGE
NÆRINGS- OG FISKERIDEPARTEMENT

Retningslinjer for sikkerhetstiltak ved elektronisk konkurransegjennomføring

Versjon 1.0, 15.02.2017

Innhold

1. INNLEDNING OG FORMÅL

Det følger av det nye regelverket om offentlige anskaffelser at kommunikasjon og informasjonsutveksling mellom oppdragsgivere og leverandørene som hovedregel skal skje skriftlig ved bruk av elektroniske kommunikasjonsmidler. Dersom elektronisk kommunikasjon skal kunne brukes, må sikkerheten være ivaretatt.

Dette dokumentet gir retningslinjer som offentlige oppdragsgivere bør følge i sine anskaffelser.

2. OVERSIKT OVER REGELVERK

2.1. Nye forskrifter om offentlige anskaffelser

Det norske regelverket for offentlige anskaffelser ble endret i 2016 gjennom endringer i lov om offentlige anskaffelser (anskaffelsesloven) og fastsettelse av tre nye forskrifter:

- Forskrift om offentlige anskaffelser (anskaffelsesforskriften),
- Forskrift om innkjøpsregler i forsyningssektoren (forsyningsforskriften),
- Forskrift om tildeling av konsesjonskontrakter (konsesjonskontraktforskriften).

En viktig endring er at kommunikasjon og informasjonsutveksling som hovedregel skal skje skriftlig ved bruk av elektronisk kommunikasjon. Kravene til elektronisk kommunikasjon er de samme for alle de tre forskriftene.

Disse retningslinjene refererer til reglene i anskaffelsesforskriftens del III, men reglene er like for alle de tre forskriftene.[1]

Muntlig kommunikasjon kan med definerte unntak anvendes. Anskaffelsesforskriften § 22-1 andre ledd regulerer hvordan muntlig kommunikasjon kan brukes i offentlige anskaffelser.

2.2. Unntak fra bruk av elektronisk kommunikasjon

Anskaffelsesforskriften § 22-4 hjemler unntak fra bestemmelsene om obligatorisk elektronisk kommunikasjon. I hovedsak gjelder dette forhold der elektronisk kommunikasjon er upraktisk eller umulig på grunn av anskaffelsens art, for eksempel på grunn av tilgang til påkrevde verktøy eller formater for det som skal leveres.

Merk imidlertid at det også finnes et sikkerhetsmessig begrunnet unntak i forskriftens § 22-4 tredje ledd:

"Oppdragsgiver kan ikke tillate bruk av elektroniske kommunikasjonsmidler til levering av tilbud hvis det er nødvendig å bruke andre kommunikasjonsmidler

a) som følge av sikkerhetsbrudd i den elektroniske kommunikasjonsløsningen eller

[1] Kravene til elektronisk kommunikasjon er regulert i anskaffelsesforskriften § 8-20, kapittel 22, § 30-1 (6) og § 31-3 (1), forsyningsforskriften kapittel 18, § 26-1 (6) og § 27-3 (1) og konsesjonskontraktforskriften kapittel 10 og § 14-1 (6).

b) fordi sensitive opplysninger ikke kan beskyttes på tilfredsstillende måte ved bruk av elektroniske verktøy og løsninger som er alminnelig tilgjengelig for leverandørene, eller som kan gjøres tilgjengelig på alternativ måte som nevnt i § 22-2 tredje ledd."

Dette betyr at dersom oppdragsgivers risikovurdering konkluderer med at sikkerheten i løsningene for elektronisk kommunikasjon ikke er tilfredsstillende, plikter oppdragsgiveren å bruke papirbasert kommunikasjon.

Dersom oppdragsgiver påberoper seg unntak fra kravet om elektronisk kommunikasjon, skal begrunnelse for avviket dokumenteres i anskaffelsesprotokollen.[2]

2.3. eIDAS-forordningen om eID og tillitstjenester

EUs forordning om elektronisk identifisering (eID) og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS-forordningen[3]) trådte i kraft i EU 1. juli 2016 og ble da gjeldende lov i alle EU-land. eIDAS krever at eID, elektronisk signatur, elektronisk segl (virksomhetssignatur) og tillitstjenester skal fungere på tvers av landegrensene i hele EØS-området[4].

Offentlige anskaffelser er «elektroniske transaksjoner i det indre marked». Bruk av eID, signaturer, segl og tillitstjenester må derfor være i henhold til eIDAS-forordningen som forventes vedtatt[5] gjeldende for Norge i løpet av 2017. Retningslinjene gir ingen gjennomgang av eIDAS-forordningens bestemmelser, men henviser til eIDAS og gjennomføringsrettsakter der dette er relevant for elektronisk kommunikasjon i offentlige anskaffelser.

2.4. Annet relevant regelverk

I henhold til § 7-3 i anskaffelsesforskriften[6] gjelder offentleglova for allmenhetens innsyn i dokumentene knyttet til en offentlige anskaffelse. En offentlig oppdragsgiver må derfor ha et bevisst forhold til offentleglova, når lovens bestemmelser om utsatt innsyn eller unntak fra innsynsrett skal brukes, og når opplysninger skal sladdes ved begjæringer om innsyn. Dokumenter skal merkes på korrekt måte dersom unntak fra innsyn eller utsatt innsyn brukes.

Anskaffelsesforskriften §§ 7-4 og 7-5[7] sier at forvaltningslovens regler om taushetsplikt og habilitet gjelder for offentlige anskaffelser.

---

[2] Jf. anskaffelsesforskriften § 25-5 andre ledd bokstav f

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[4] EØS-området består av EUs medlemsland og de tre EØS-landene Norge, Island og Liechtenstein. eIDAS er en EØS-relevant forordning. Det betyr at eIDAS tas inn i EØS-avtalen og gjelder for hele EØS-området.

[5] https://www.regjeringen.no/no/dokumenter/gjennomforing-av-eus-forordning-om-elektronisk-identifisering-eid-og-tillitstjenester-for-elektroniske-transaksjoner-i-det-indre-marked---horing/id2464892/

[6] Tilsvarende bestemmelse i forsyningsforskriften § 7-2

[7] Tilsvarende bestemmelser i forsyningsforskriften §§ 7-3 og 7-4 og konsesjonskontraktforskriften §§ 7-2 og 7-3

Enkelte anskaffelser kan medføre at sensitive personopplysninger inkluderes i anskaffelsesdokumentene eller i tilbudene. I slike tilfeller må elektronisk kommunikasjon beskyttes i henhold til personopplysningsloven med forskrifter. Eventuell innsamling og lagring av personopplysninger i forbindelse med en anskaffelse, for eksempel om ansatte hos tilbydere, skal også være i henhold til personopplysningsloven.

For øvrig kan anskaffelser innen forskjellige sektorer være underlagt krav fra sektorens regelverk.

3. ANSKAFFELSESREGELVERKETS KRAV TIL INFORMASJONSSIKKERHET

3.1. Risikobasert fastsettelse av sikkerhetstiltak

Intensjonen i anskaffelsesforskriften er at informasjonssikkerhet skal baseres på risikovurderinger og ikke på normative krav om at bestemte tiltak eller mekanismer alltid skal brukes. Spesielt viktig er det at leverandører ikke pålegges strenge sikkerhetstiltak med mindre dette er nødvendig.

Oppdragsgiver skal i konkurransegrunnlaget angi krav til leverandørens bruk av signatur, eID og andre sikkerhetsmekanismer[8]. Det er oppdragsgiver som bestemmer sikkerhetsnivået, men oppdragsgiver bør i sine risikovurderinger også se på risiko fra leverandørens perspektiv siden innholdet i forespørsler om å delta i konkurransen, tilbud e.l. i stor grad er leverandørens informasjon.

Oppdragsgiver kan videre stille krav om at leverandøren bruker løsninger som i tilfredsstillende grad sannsynliggjør hvem som har levert forespørsel/tilbud, og som i tilfredsstillende grad knytter leverandøren til innholdet i forespørselen/tilbudet[9]. Slike løsninger vil i praksis innebære bruk av eID og/eller former for elektronisk signatur eller elektronisk segl. Oppdragsgiver kan etter en risikovurdering kreve at leverandøren bruker «avansert elektronisk signatur» som definert av eIDAS[10][11].

Når det gjelder spesifisering av sikkerhetskrav i konkurransegrunnlaget, legger retningslinjene følgende til grunn:

- Normalsituasjonen er at oppdragsgiver baserer seg på sentral tilrettelegging (se punktene 4.1 til 4.4), og at oppdragsgivers risikovurdering konkluderer med at dette gir tilstrekkelig sikkerhet. En trenger da ikke å spesifisere eksplisitte sikkerhetskrav i konkurransegrunnlaget.
- Punkt 5.4.3 identifiserer ett ekstra sikkerhetstiltak som oppdragsgiver kan stille krav om: Bruk av «avansert elektronisk signatur» fra leverandøren. Dersom dette kreves, må det spesifiseres eksplisitt i konkurransegrunnlaget.

[8] Jf. anskaffelsesforskriften § 22-5 tredje ledd
[9] Jf. anskaffelsesforskriften § 22-5 andre ledd
[10] Jf. anskaffelsesforskriften § 22-5 femte ledd
[11] Inntil eIDAS-forordningen er innført i norsk lov er begreper knyttet til elektronisk signatur definert av e-signaturloven.

- Dersom oppdragsgiver ikke baserer seg på sentral tilrettelegging (se punkt 4.5), må oppdragsgiver selv forsikre seg om at de løsninger som velges ivaretar sikkerhetskravene i anskaffelsesforskriften. Eventuelle spesifikke tiltak som leverandører må oppfylle, må angis i konkurransegrunnlaget i den enkelte konkurranse. Retningslinjene beskriver ikke hvordan slike krav skal formuleres da dette vil kunne variere avhengig av hvilken løsning oppdragsgiver har valgt for å gjennomføre sine anskaffelser.

3.2. Kunngjøringsfasen

Tilgang til konkurransegrunnlaget og melding av interesse fra leverandør skal ikke kreve bruk av elektronisk signatur eller elektroniske identifikasjonsbevis (eID)[12]. Konkurransegrunnlaget skal normalt være fritt og åpent tilgjengelig på DOFFIN, og på TED der det er relevant.

Et konkurransegrunnlag kan i enkelte tilfeller inneholde fortrolige opplysninger, eksempelvis ved anskaffelser av helse- og sosialtjenester. Anskaffelsesforskriften § 14-3 tredje ledd inneholder derfor en unntaksbestemmelse. Dersom det ikke kan gis ubegrenset tilgang til konkurransegrunnlaget, skal oppdragsgiver angi hvordan leverandører kan få tilgang, og hvilke tiltak som er nødvendige for å sikre fortrolighet. Kapittel 6 nedenfor gir anbefalinger for informasjonssikkerhet for anskaffelser der det ikke kan gis ubegrenset tilgang til konkurransegrunnlaget.

3.3. Konkurransefasen

Anskaffelsesforskriften har i § 22-3 egne bestemmelser om oppdragsgivers håndtering av forespørsler om å delta i konkurransen og tilbud. Det stilles krav om at disse skal beskyttes mot endringer og mot uautorisert innsyn under overføring og lagring. Ingen skal ha tilgang til innholdet før fristen for mottak er utløpt. Tidspunkt for hendelser (mottak, åpning) skal kunne fastsettes nøyaktig. Brudd eller forsøk på brudd på sikkerheten skal i tilfredsstillende grad kunne spores.

Kontrakt kan inngås elektronisk og signeres på den måten partene finner hensiktsmessig. Difis fellesløsning for signering[13] kan brukes hvis kontrakten skal signeres med avansert elektronisk signatur.

En oppdragsgiver skal avvise et tilbud som ikke kan åpnes eller leses. Dersom dette skyldes feil ved krypteringen slik at oppdragsgiver ikke kan dekryptere innholdet, anbefales oppdragsgiver å undersøke om nødvendige nøkler for dekryptering kan framskaffes.

Andre avvik fra krav til sikkerhet, eID og signatur krever normalt ikke avvisning. Eksempler er at leverandøren har latt være å kryptere innholdet, at elektroniske signaturer ikke lar seg verifisere, eller at krav om bruk av avansert elektronisk signatur ikke er oppfylt.

[12] Jf. anskaffelsesforskriften § 22-5 første ledd
[13] https://www.difi.no/fagomrader-og-tjenester/digitale-felleslosninger/signeringstjenesten

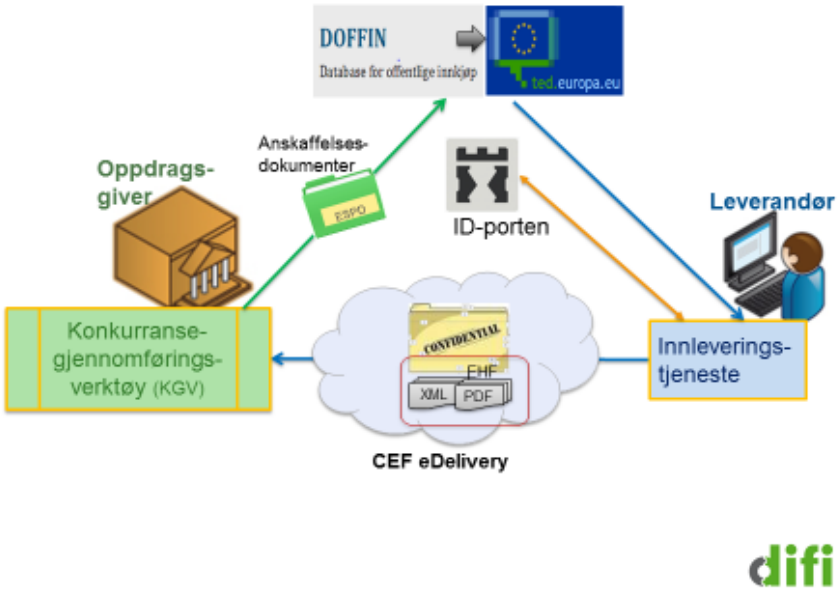
4. SENTRAL TILRETTELEGGING FOR ELEKTRONISK KOMMUNIKASJON

4.1. Anbefalt modell for elektronisk kommunikasjon i konkurransefasen

I den anbefalte norske modellen (Figur 1) skal markedet, basert på sentral tilrettelegging, levere løsninger hvor oppdragsgivere og leverandører elektronisk kan kommunisere med bruk av hver sin tjeneste. Modellen forutsetter at oppdragsgiveren må ha inngått avtale med en tjeneste for konkurransegjennomføring (KGV-tjeneste), og leverandøren må ha en avtale med en innleveringstjeneste. Avtalene må regulere ansvarsforhold og tjenestekvalitet, inkludert informasjonssikkerhet.

Både KGV-tjenesten og innleveringstjenesten må være tilkoplet den felles europeiske infrastrukturen CEF eDelivery som sørger for sikker forsendelse av dokumenter over Internett.

Dette er den samme modellen som i dag brukes for ordre og faktura, og innebærer at leverandøren kan velge tjenestetilbyder for innlevering uavhengig av hvilken KGV-tjeneste oppdragsgiver har valgt for sin konkurransegjennomføring. Figur 1 viser også hvordan DOFFIN og TED brukes for kunngjøring, og hvordan ID-porten kan brukes av en innleveringstjeneste for å identifisere leverandøren og om nødvendig signere tilbudet.



Figur 1: Uavhengige tjenestetilbydere for oppdragsgiver og leverandør

4.2. Sentral tilrettelegging for anbefalt modell

Direktoratet for forvaltning og IKT (Difi) tilrettelegger sentralt slik at den anbefalte modellen for elektronisk kommunikasjon enkelt skal kunne tas i bruk. Siden risikovurderinger og valg av tiltak for informasjonssikkerhet vanligvis ikke er kjernekompetanse hos offentlige innkjøpere, er et vesentlig element av denne tilretteleggingen å forenkle oppdragsgiveres ivaretakelse av informasjonssikkerhet, primært gjennom to tiltak:

- En veiledningspakke for anskaffelse av KGV-tjenester med blant annet en kravspesifikasjon som inneholder relevante sikkerhetskrav (se punkt 4.3 nedenfor).
- Bruk av CEF eDelivery, som er en felles, europeisk infrastruktur for sikker og pålitelig meldingskommunikasjon (se punkt 4.4 nedenfor). Krav til bruk av CEF eDelivery er innarbeidet i veiledningspakken for anskaffelse av KGV.

Det er den enkelte oppdragsgiver som må sørge for å anskaffe en KGV-løsning i tråd med den sentrale tilretteleggingen, se punkt 4.5 nedenfor vedrørende alternativer til dette.

Difis sentrale tilrettelegging fritar ikke oppdragsgiver for i den enkelte konkurranse å vurdere om det er behov for utvidede sikkerhetstiltak.

Normalt vil leverandøren bruke en tjenestetilbyder (innleveringstjeneste) for å sende tilbud i offentlige anskaffelser. Det er leverandørens ansvar å velge en innleveringstjeneste som tilbyr tilstrekkelig beskyttelse mot uønsket innsyn, uønskede endringer og andre trusler inntil tilbudet er mottatt/levert hos oppdragsgiver. Oppdragsgiver kan ikke holdes ansvarlig for manglende sikkerhet i leverandørens egne systemer eller i leverandørens innleveringstjeneste.

Retningslinjene omtaler derfor *kun* sikkerhet i oppdragsgivers KGV-tjeneste, samt overføringen *mellom* leverandørens innleveringstjeneste og KGV-tjenesten.

4.3. Veileder for anskaffelse av Konkurransegjennomføringsverktøy (KGV)

Oppdragsgivers avtale med KGV-tjenesten må stille krav som i tilfredsstillende grad ivaretar sikkerhetskravene i anskaffelsesforskriften. Dette gjelder:

- Sikkerhet for at leverandørens identitet er korrekt, og at det innleverte tilbud eller forespørsel om å delta i konkurransen er utvetydig knyttet til leverandøren.

- Sikkerhet for at tilbudet eller forespørselen om å delta i konkurransen er beskyttet mot uautorisert innsyn og uautoriserte endringer under mottak og lagring, både overfor eksterne angripere og innsideangrep fra KGV-tjenestens personell eller oppdragsgivers personell. Som del av dette sikkerhet for at ingen har tilgang til innholdet før tilbudsfristen er gått ut.

- Sporbarhet av handlinger knyttet til dokumentene inkludert fastsettelse av tid for hendelser.

Difi har publisert en veiledningspakke for anskaffelse av standard KGV.[14] De anbefalte "skal-kravene" i pakkens spesifikasjonsskjema ivaretar kravene til grunnleggende informasjonssikkerhet i KGV-løsningene. Retningslinjene peker i punkt 5 på hvilke sikkerhetskrav som blir ivaretatt dersom KGV-leverandørens løsning oppfyller veilederens krav.

4.4. CEF eDelivery, sikker transport over internett

Den anbefalte modellen krever sikker og pålitelig kommunikasjon mellom leverandørens og oppdragsgiverens systemer, det vil si vanligvis mellom innleveringstjeneste og KGV-tjeneste. Difi forvalter norsk tilknytning til PEPPOL-profilen av CEF eDelivery[15] (PEPPOL eDelivery). PEPPOL eDelivery benyttes for flere formål i Norge og generelt i mange løsninger for elektronisk handel i Europa.

Anbefalt modell for elektronisk kommunikasjon er at alle tjenestetilbydere er tilknyttet PEPPOL eDelivery. Retningslinjene legger til grunn at PEPPOL eDelivery brukes. Merk at retningslinjene refererer til bruk av CEF eDelivery, men i praksis vil dette bety PEPPOL eDelivery.

4.5. Alternativer til anbefalt modell

4.5.1. Oppdragsgiver og/eller leverandør bruker interne systemer

Selv om den normale situasjonen vil være at både oppdragsgiver og leverandør benytter seg av tjenestetilbydere, kan den ene eller begge av dem velge å håndtere hele prosessen i interne systemer. En stor oppdragsgiver kan ha egne systemer for innkjøp, og en stor leverandør kan ha interne systemer for tilbudsinnlevering.

Slike aktører vil normalt være underlagt samme krav som en tjenestetilbyder med hensyn til tilknytning til CEF eDelivery og støtte for nødvendige anskaffelsesprosesser og krav til informasjonssikkerhet. Bruk av andre former for kommunikasjon enn CEF eDelivery frarådes.

Retningslinjene gir i liten grad hjelp til oppdragsgivere som velger å bruke helt proprietære løsninger. Punkt 5 kan brukes som grunnlag for risikovurderinger, men oppdragsgiver må så på egenhånd dokumentere hvordan identifisert risiko er håndtert.

4.5.2. Oppdragsgiver og leverandør bruker begge oppdragsgivers løsning

En del oppdragsgivere benytter i dag en KGV-løsning (KGV-tjeneste fra markedet eller interne systemer) hvor en leverandør må logge seg på oppdragsgivers løsning og

[14] https://www.anskaffelser.no/oppdragsgivere/konkurransegjennomforing-og-kgv/anskaffelse-av-kgv
[15] CEF står for Connecting Europe Facility. CEF Digital er innsatsområdet for elektronisk kommunikasjon og digitale tjenester, blant annet sikker og pålitelig meldingskommunikasjon. https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/(Building%20Block%20DSI_IntroDocument)%20(eDelivery)%20(v1%2002).pdf

levere sitt tilbud eller forespørsel om deltakelse direkte i KGV-løsningen. En slik løsning har ikke behov for sikker meldingsutveksling som beskrevet i punkt 4.4, men all risiko ligger på oppdragsgiver siden det kreves at leverandøren benytter oppdragsgivers løsning med det sikkerhetsoppsettet denne løsningen måtte ha.

Oppdragsgivere som har eksisterende KGV-avtaler der veiledningspakkens «skal-krav» knyttet til sikkerhet ikke er dekket, må selv sikre at kravene blir ivaretatt. Ved nye anskaffelser av KGV-tjenester anbefales det sterkt å legge anbefalt modell og malverket for KGV-anskaffelser til grunn.

Retningslinjene gir ikke utførlig veiledning for situasjonen der både oppdragsgiver og leverandør bruker samme KGV-tjeneste siden potensiell risiko da vil variere fra løsning til løsning. Punkt 5 gir imidlertid veiledning om risikovurderinger og hvilke spørsmål oppdragsgiver må stille til den valgte leverandøren av KGV-tjeneste for å sikre at risiko er tilfredsstillende håndtert.

5. RISIKOVURDERING OG SIKKERHETSTILTAK FOR ELEKTRONISK KOMMUNIKASJON

5.1. Innledning

Informasjonssikkerhet beskrives ut fra egenskapene **konfidensialitet** (beskyttelse mot uautorisert innsyn), **integritet** (beskyttelse mot uautoriserte endringer og sletting av informasjon) og **tilgjengelighet** (å sikre tilgang til informasjon ved behov for tilgang)[16]. Sikkerhetstiltak kan beskytte både mot tilsiktede handlinger og tilfeldige, uønskede hendelser. For eksempel vil integritetsbeskyttelse av et dokument beskytte både mot endringer som skyldes et angrep, og endringer som skyldes tilfeldige feil i IT-systemer. Trusler mot tilgjengelighet er i hovedsak feil og mangler, men tilsiktede angrep mot systemer kan også gjøre dem utilgjengelige eller påvirke ytelsen negativt.

For offentlige anskaffelser legger retningslinjene til ytterligere to egenskaper: **Identitet** (knytning av leverandøren til tilbud/forespørsel om deltakelse[17]) og **sporbarhet** (sporing av brudd eller forsøk på brudd på sikkerheten). Identitet inkluderer vurdering av eventuelle behov for elektronisk signatur.

For hver sikkerhetsegenskap beskrives kort i det følgende:

- Hvilke uønskede hendelser kan oppstå ved elektronisk kommunikasjon i en offentlig anskaffelse.
- Hva er sannsynligheten for at en hendelse inntreffer.
- Hvor alvorlig er konsekvensen om hendelsen inntreffer.
- I hvilket omfang vil den sentrale tilretteleggingen ivareta sikkerhetstiltak som beskytter mot hendelsen.
- Kan det være behov for ytterligere sikkerhetstiltak.

[16] http://internkontroll.infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet
[17] I sikkerhetsterminologi brukes vanligvis begrepet «autentisitet».

Risiko forbundet med en uønsket hendelse er gitt av kombinasjonen av sannsynlighet og konsekvens. Det er viktig å innse at uansett hvilke sikkerhetstiltak en innfører, vil det alltid finnes en restrisiko. Et element i risikovurderinger er derfor hvilken risiko en er villig til å akseptere.

Hvis en risikovurdering konkluderer med at tilgjengelige sikkerhetstiltak ikke er tilstrekkelige, må oppdragsgiver vurdere om unntaksbestemmelsene for elektronisk kommunikasjon (se punkt 2.2) gjelder.

Dette kapitlet bruker i en del sammenhenger *innlevering av tilbud* i teksten. Merk at all kommunikasjon som er omfattet av regelverket, skal dekkes av risikovurderinger og sikkerhetstiltak, for eksempel kunngjøring, forespørsel om å delta i konkurransen og innlevering av tilbud eller dokumentasjonsbevis.

5.2. Sikkerhet som følger av basiskrav til informasjonssikkerhet i offentlige virksomheter

Alle offentlige virksomheter er pålagt å ha internkontroll på informasjonssikkerhetsområdet basert på anerkjente standarder, se eforvaltningsforskriften § 15. Difi publiserer veiledningsmateriale[18] for slik internkontroll.

Retningslinjene legger til grunn at alle offentlige virksomheter har internkontroll, inkludert risikovurdering[19] og risikohåndtering[20], på plass. Virksomhetsintern sikkerhet i forbindelse med offentlige anskaffelser antas derfor å være ivaretatt av den eksisterende internkontrollen.

Internkontrollen skal ha rutiner for håndtering av brudd på informasjonssikkerhet. Retningslinjene legger til grunn at disse rutinene også dekker brudd på informasjonssikkerhet i anskaffelser.

5.3. Sikkerhet fra sentral tilrettelegging

Den sentrale tilretteleggingen for elektronisk kommunikasjon (se kapittel 4) har innebygget basis sikkerhetstiltak som er ment å være tilstrekkelige for de aller fleste anskaffelser. Tilretteleggingen understøtter også noen valgbare, ekstra sikkerhetstiltak.

Det er oppdragsgivers ansvar å vurdere om den enkelte anskaffelse er tilstrekkelig dekket av sentral tilrettelegging. Oppdragsgivere som ikke bruker den sentrale tilretteleggingen, er selv ansvarlig for å få på plass nødvendige sikkerhetstiltak.

[18] http://internkontroll.infosikkerhet.difi.no
[19] http://internkontroll.infosikkerhet.difi.no/risikovurdering
[20] http://internkontroll.infosikkerhet.difi.no/risikohandtering

5.4. Risikovurdering for leverandørens identitet og for signatur

5.4.1.Risikovurdering uten tiltak

Anskaffelsesforskriften sier at oppdragsgiver *kan* kreve at leverandørene ved levering av tilbud eller forespørsel om deltagelse bruker løsninger som gir tilfredsstillende sikkerhet for å sannsynliggjøre hvilken leverandør som har levert den enkelte forespørsel eller tilbud. De fleste oppdragsgivere vil i anskaffelser over en viss størrelse ønske å be om dette.

Oppdragsgiver *kan* for ytterligere sikkerhet kreve bruk av elektronisk signatur, elektronisk segl (virksomhetssignatur) eller elektronisk identitetsbevis (eID).

Hendelse	**Sannsynlighet uten tiltak**	**Konsekvens**
Falskt tilbud sendt av en annen enn den påståtte leverandøren.	Meget lav	Kan være stor
Leverandøren vedkjenner seg ikke å ha sendt tilbudet.	Lav	Kan være stor

Dersom en leverandør ikke vedkjenner seg et tilbud, kan årsaken enten være at personen som har sendt tilbudet har gjort dette i strid med sine fullmakter hos leverandøren, eller at leverandøren av andre grunner ikke lenger ønsker å vedkjenne seg tilbudet. Det skal imidlertid svært mye til før en leverandør kan frasi seg ansvaret for at et levert tilbud er sendt. Bevisbyrden påligger i slike tilfeller leverandøren.

Konsekvensen av at en leverandør benekter å ha levert et tilbud vil være relativt liten hvis dette blir avdekket tidlig. Hvis det avdekkes senere kan konsekvensen være stor hvis oppdragsgiver må gjennomføre konkurransen på nytt.

Dersom oppdragsgiver lider tap på grunn av feil gjort av leverandørens innleveringstjeneste, må oppdragsgiver i utgangspunktet holde leverandøren ansvarlig.

5.4.2.Sikkerhetstiltak fra sentral tilrettelegging

Ved bruk av anbefalt modell for elektronisk kommunikasjon (se punkt 4.1) plikter leverandørens innleveringstjeneste som betingelse for å kunne benytte ID-porten og for å knytte seg til CEF eDelivery å:

- Oppgi leverandørens identitet (i Norge organisasjonsnummer) til oppdragsgiveren,
- Gå god for at leverandøren (det vil vanligvis si en person tilknyttet leverandøren) er autentisert (pålogget) i innleveringstjenesten for innsending av tilbudet, og
- Gå god for at leverandøren eksplisitt har bedt om at tilbudet blir sendt.

Et viktig poeng med dette aspektet i den sentrale tilretteleggingen er at det skal kunne skapes en tilstrekkelig knytning mellom leverandør og tilbud uten at leverandøren skal

trenge å bruke en elektronisk signatur ved hver eneste innlevering av tilbud eller forespørsel om å delta i konkurranse.

Sentral tilrettelegging skal også dekke integritet og sporbarhet, egenskaper som er nødvendige for identitet (se punkt 5.5 og 5.8).

5.4.3.Ekstra sikkerhetstiltak

Sentral tilrettelegging innebærer at oppdragsgiver stoler på at innleveringstjenestens formidling av leverandørens identitet er korrekt, og at oppdragsgiver stoler på at tilbudet er sendt i henhold til nødvendige fullmakter. Restrisiko knyttet til hendelsene som er beskrevet i punkt 5.4.1 over, bør være akseptabel for de aller fleste anskaffelser, og det skal normalt ikke være behov for ytterligere sikkerhetstiltak.

Dersom oppdragsgiver vil ha ytterligere sikkerhet for leverandørens identitet, må oppdragsgiver få bekreftet leverandørens identitet og vedståelse av tilbudet gjennom en «avansert elektronisk signatur» fra leverandøren selv. Dersom dette kreves, må det spesifiseres i konkurransegrunnlaget, se punkt 3.1.

En «avansert elektronisk signatur» gir en enda sikrere kopling mellom personen som signerer, og dokumentet som blir signert, uavhengig av innleveringstjenesten. Eventuelle endringer etter at dokumentet er signert vil ugyldiggjøre signaturen. Normalt vil en bare kreve at tilbudsbrevet signeres, men det er også mulig å stille krav om at alle dokumenter i tilbudet skal signeres. Difi legger til rette for at innleveringstjenester skal kunne bruke Difis signeringstjeneste.

Avansert elektronisk signatur bør bare vurderes ved tilbud av stor verdi eller med andre spesielle sikkerhetsbehov. Krav om signering hever terskelen for å levere tilbud.

Dersom avansert elektronisk signatur kreves, skal signaturer være med sertifikat fra utsteder som er registrert på tillitsliste[21] over tilbydere av tillitstjenester. I Norge betyr dette i dag signatur med BankID, Buypass eID eller Commfides ID. Tilsvarende signatur ("avansert signatur med kvalifisert sertifikat" som definert av eIDAS-forordningen) fra andre EØS-land skal aksepteres. Signaturformat skal være i henhold til gjennomføringsrettsakt for eIDAS[22]. Kun "basis signaturformat", det vil si uten bruk av tidsstempel, skal kreves.

En oppdragsgiver kan velge å formulere krav slik at avansert elektronisk segl (virksomhetssignatur) fra leverandøren kan brukes i stedet for signatur fra en fysisk person. Oppdragsgiver bør ikke stille obligatorisk krav om bruk av elektronisk segl siden det ikke kan forutsettes at leverandører kan oppfylle et slikt krav. I Norge utsteder både Buypass og Commfides sertifikater for elektronisk segl. Difis signeringstjeneste tilrettelegger ikke i dag for elektroniske segl.

---

[21] I Norge er Nasjonal Kommunikasjonsmyndighet ansvarlig for denne listen, se http://www.nkom.no/teknisk/elektronisk-signatur/kvalifisert-sertifikat/tl-liste-trusted-list-av-norge

[22] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

5.5. Risikovurdering for integritet

5.5.1.Risikovurdering uten tiltak

Anskaffelsesforskriften sier at oppdragsgiver skal sikre at tilbud og forespørsler om å delta i konkurransen beskyttes mot endringer under overføring og lagring. Endringer kan skyldes både tilsiktede hendelser og tilfeldige feil.

Hendelse	**Sannsynlighet uten tiltak**	**Konsekvens**
Tilbudet er endret under transport mellom leverandør og oppdragsgiver	Lav til middels	Meget stor
Tilbudet er endret under mottak og lagring hos oppdragsgiver	Middels	Meget stor
Tilbudet blir borte under transport mellom leverandør og oppdragsgiver	Lav til middels	Meget stor
Tilbudet slettes ved mottak eller lagring hos oppdragsgiver	Middels	Meget stor

Sannsynligheten for at noe skal skje under transport avhenger av hvilken type nettverkstjeneste som benyttes for overføring. Sannsynligheten for at noe skal skje under mottak og lagring kan være større. Både interne personer (i vanvare eller utro tjenere) og eksterne angripere kan være involvert.

Konsekvenser av brudd på integritet kan være meget store siden det kan medføre avvisning av tilbud og/eller tildeling av kontrakt på feil grunnlag.

5.5.2.Sikkerhetstiltak fra sentral tilrettelegging

Sentral tilrettelegging sikrer at alle endringer fra tilbudet er sendt og til det er mottatt hos oppdragsgiver (i KGV-tjenesten) vil bli oppdaget. Transportinfrastrukturen skal garantere at tilbudet kommer fram, eller at leverandøren får klare feilmeldinger dersom for eksempel mottakeren ikke kan nås. Leverandøren kan be om å få en kvittering (bevis) på at det som er levert til oppdragsgiver, er det samme som ble sendt.

5.5.3.Behov for ytterligere sikkerhetstiltak

Sentral tilrettelegging anses å gi tilstrekkelig integritetsbeskyttelse under transport av alle tilbud.

For mottak og lagring forutsettes oppdragsgiver og leverandører av KGV-tjenester å ha internkontroll for informasjonssikkerhet på plass. Dette må omfatte gode rutiner for

tildeling av rettigheter til å åpne, se og arbeide med mottatte tilbud. Det anbefales at oppdragsgiver sikrer at mottatte tilbud "fryses", og at arbeid som kan medføre endringer, gjøres på arbeidskopier.

Merk at dersom enkeltdokumenter i tilbudet har avansert elektronisk signatur eller avansert elektronisk segl, vil signaturen/seglet gi en ekstra sikkerhet for at endringer vil bli oppdaget.

5.6. Risikovurdering for konfidensialitet

5.6.1. Risikovurdering uten tiltak

Anskaffelsesforskriften sier at oppdragsgiver skal sikre at tilbud og forespørsler om å delta i konkurransen holdes fortrolig og beskyttes mot uautorisert innsyn under overføring og lagring.

Hendelse	Sannsynlighet uten tiltak	Konsekvens
Uvedkommende får tilgang til innhold i tilbudet under transport mellom leverandør og oppdragsgiver.	Lav til middels	Kan være meget stor
Uvedkommende får tilgang til innhold i tilbudet under lagring hos oppdragsgiver.	Middels	Kan være meget stor
Innsyn i tilbud før tidspunkt for åpning.	Middels	Kan være meget stor

Sannsynligheten for at noe skal skje under transport avhenger av kommunikasjonskanalen som benyttes for overføring. Sannsynligheten for at noe skal skje under lagring kan være større. Både interne personer (i vanvare eller utro tjenere) og eksterne angripere kan være involvert.

Konsekvenser av uautorisert innsyn avhenger av hvem som får innsyn. Dersom dette er en "tilfeldig" utenforstående, kan konsekvensen være liten, men i andre tilfeller kan uautorisert innsyn ha meget store konsekvenser.

5.6.2. Sikkerhetstiltak fra sentral tilrettelegging

Sentral tilrettelegging sikrer at sendingen er kryptert ende-til-ende mellom leverandøren og helt fram til KGV-tjenesten slik at en i praksis kan se bort fra muligheten for innsyn under transport. Dersom KGV-tjenesten dekrypterer på tidspunkt for åpning, vil også muligheten for innsyn før tidspunkt for åpning være meget begrenset.

Veiledningspakken for anskaffelse av KGV har sikring av konfidensialitet som et "skal-krav". Logger i KGV-tjenesten skal kunne vise hvem som har hatt tilgang, noe som vil

fungere forebyggende på eventuell utroskap hos oppdragsgiver og dennes tjenesteleverandør.

5.6.3.Behov for ytterligere sikkerhetstiltak

Sentral tilrettelegging anses å gi tilstrekkelig konfidensialitetsbeskyttelse for transport av tilbud. Det skal normalt ikke være behov for ytterligere tiltak.

Merk at sentral tilrettelegging ikke krypterer/skjuler adresseringsinformasjon slik at det er mulig (men ikke enkelt) for utenforstående å finne ut hvem som sender til hvem, og på hvilket tidspunkt. Normalt er dette en akseptabel risiko ved tilbudsinnlevering.

5.7. Risikovurdering for tilgjengelighet

5.7.1.Krav og risikovurdering før tiltak

Ethvert IT-system kan ha feil og mangler som medfører utilgjengelighet eller redusert ytelse, eller det kan bli utsatt for bevisste angrep som har samme effekt. En spesiell kategori angrep er "nektelse av tjeneste" der angriperens formål er spesifikt å blokkere tilgang til et system.

For tilbud i offentlige anskaffelse er det viktig at involverte systemer har høy tilgjengelighet spesielt på tidspunkt for innleveringsfrister.

Hendelse	**Sannsynlighet uten tiltak**	**Konsekvens**
Tilbud kan ikke leveres på grunn av manglende tilgjengelighet i nettverk.	Middels	Kan være meget stor
Tilbud kan ikke leveres på grunn av manglende tilgjengelighet hos oppdragsgiver.	Middels	Liten til stor

Oppdragsgiver kan ikke holdes ansvarlig dersom tilbud ikke kan leveres på grunn av feil ved nettverk eller systemer på leverandørens side, for eksempel utilgjengelig "postkasse" eller innleveringstjeneste. Dette er derfor ikke tatt med som hendelse.

Et tilbud skal ansees som levert når det er mottatt i KGV-tjenestens "postboks" for CEF eDelivery. Dersom denne postboksen ikke er tilgjengelig på tidspunktet for en tilbudsfrist, og leverandører av den grunn ikke får levert tilbud i tide, må oppdragsgiver normalt gi utsatt frist.

Oppdragsgiver må også vurdere behovet for utsatt frist dersom hele eller deler av CEF eDelivery infrastrukturen er utilgjengelig.

Dersom oppdragsgiver ikke benytter den sentrale tilretteleggingen, og leverandøren er pålagt å bruke oppdragsgivers løsning for å lage og levere sitt tilbud (se punkt 4.5.2), er oppdragsgiver ansvarlig for at løsningen er tilgjengelig slik at leverandøren kan levere. Dersom løsningen er utilgjengelig på tidspunkt for en tilbudsfrist, anbefales

oppdragsgiver å vurdere kortvarig utsettelse av innleveringsfristen dersom dette ikke fører til forskjellsbehandling av potensielle leverandører. Det forutsettes tydelig varsling av utsettelsen til alle berørte leverandører.

5.7.2.Basis sikkerhetstiltak som er inkludert i sentral tilrettelegging

CEF eDelivery med "postkasser" er en infrastruktur med høy tilgjengelighet og pålitelighet, men feil kan selvsagt ikke utelukkes 100 %.

5.7.3.Ekstra sikkerhetstiltak

Risikoen for utilgjengelighet ved bruk av CEF eDelivery vil vanligvis vurderes som akseptabel, slik at ingen ytterligere tiltak er nødvendig. Som en del av oppdragsgivers system for internkontroll, se punkt 5.2, forutsettes det at oppdragsgiver har en plan for håndtering av hendelser som medfører manglende eller utilstrekkelig tilgjengelighet på tidspunkt for tilbudsinnlevering

Oppdragsgiver må vurdere om det kan gis utsatt frist for levering. Lengden på utsettelsen kan ikke være for lang da dette kan endre betingelsene for konkurransen. Alle som er berørt av hendelsen må varsles.

5.8. Sporbarhet

5.8.1.Krav og risikovurdering før tiltak

Anskaffelsesforskriften sier at oppdragsgiver i enhver konkurranse i tilfredsstillende grad skal sikre at overtredelse eller forsøk på overtredelse av sikkerhetsbestemmelsene klart kan spores. Tidspunkt for mottak og åpning av forespørsel om deltagelse og tilbud skal kunne fastslås nøyaktig.

Manglende sporing utgjør ikke noen sikkerhetsrisiko i seg selv, men kan medføre at sikkerhetsbrudd ikke oppdages eller ikke kan bevises. Sporbarhet som forutsetning for sporing av (forsøk på) brudd på sikkerhet er derfor omtalt under de enkelte, andre sikkerhetsegenskapene.

Hendelse	**Sannsynlighet uten tiltak**	**Konsekvens**
Tilbud er levert for sent, men påstås levert i tide.	Middels	Kan være meget stor
Tilbud er levert i tide, men påstås levert for sent.	Lav	Kan være meget stor
Tilbud åpnes for tidlig.	Lav	Liten til stor

Feil tidspunkt for mottak vil vanligvis vurderes som lite sannsynlig, men konsekvensen av feilaktig avvisning av et tilbud som egentlig var levert i tide, er stor. Konsekvensen av

feilaktig å godta et tilbud som egentlig var levert for sent, kan også være stor. Hendelser kan skyldes tilfeldige feil i systemene som brukes, men også bevisste handlinger som at en oppdragsgiver bevisst påstår at et tilbud ble levert for sent.

5.8.2. Basis sikkerhetstiltak som er inkludert i sentral tilrettelegging

Tidspunkt for mottak er bestemt til å være tidspunkt tilbudet er mottatt i KGV-tjenestens "postboks" for CEF eDelivery. CEF eDelivery logger sending og mottak av meldinger, men ikke meldingsinnhold. Kombinert med logging i innleveringstjenesten og i KGV-tjenesten betyr dette at en melding skal kunne spores fra sending til mottak.

CEF eDelivery skal på forespørsel kunne avgi bevis for når en gitt melding er levert til KGV-tjenestens "postboks", det vil si tidspunktet for levering av tilbud. Oppdragsgiver og leverandør kan uavhengig av hverandre be om å få et slikt bevis.

Det forutsettes at alle involverte systemer har korrekte klokker. I CEF eDelivery vil unormale tidsangivelser bli oppdaget, som for eksempel at det oppgis fra en "postboks" at en melding tilsynelatende er mottatt på et langt senere eller tidligere tidspunkt enn normalt.

Åpning skjer internt i KGV-tjenesten, og tidspunktet må derfor dokumenteres av KGV-tjenesten.

5.8.3. Ekstra sikkerhetstiltak

Det ansees ikke å være noe ekstra behov for tiltak spesifikt for sporbarhet, ut over tilstrekkelig, sikker logging i alle involverte systemer.

6. ANBEFALINGER OM TILGANG TIL KONKURRANSEGRUNNLAG SOM INNEHOLDER FORTROLIGE OPPLYSNINGER

Kunngjøring skal normalt inneholde konkurransegrunnlaget og være åpent tilgjengelig på DOFFIN, og TED når det er relevant. Konkurransegrunnlaget kan imidlertid ikke være åpent tilgjengelig dersom det inneholder fortrolige opplysninger, jf. anskaffelsesforskriften § 14-3 tredje ledd. I slikt tilfelle skal kunngjøringen på DOFFIN og TED ikke inneholde konkurransegrunnlaget, men kun informasjon om hvordan leverandører kan få tilgang til dette.

Konkurransegrunnlaget kan publiseres på oppdragsgivers egne nettsider, eller fra KGV-tjenesten, eller leveres ut på annen måte. Følgende anbefales:

- Leverandører bør levere taushetserklæring før det gis tilgang til konkurransegrunnlaget. Erklæringen bør inneholde forpliktelse fra leverandøren til å lagre informasjonen sikkert enten dette er i egne systemer eller i en innleveringstjeneste (jf. anskaffelsesforskriften § 7-4).

- Tilgang til konkurransegrunnlaget bør begrenses til autorisert(e) person(er) hos leverandøren, og alle disse personene bør ha avgitt taushetserklæring. Oppdragsgivers ordinære rutiner og skjema for håndtering av personsensitive opplysninger anbefales brukt. Taushetserklæring *kan* avgis elektronisk. Dersom oppdragsgiver krever avansert elektronisk signatur på taushetserklæringen, kan Difis fellesløsning for signering brukes[23].
- Det kan være nødvendig å verifisere at personen(e) som signerer taushetserklæringene har de nødvendige fullmakter hos leverandøren.
- Tilgang til konkurransegrunnlaget bør kun gis over en elektronisk kommunikasjonskanal dersom kommunikasjonskanalen er kryptert.

[23] https://www.difi.no/fagomrader-og-tjenester/digitale-felleslosninger/signeringstjenesten