

VEDLEGG 4 TJENESTEUTSETTING

Tjenesteutsetting

Tjenesteutsetting betyr at kommunen anskaffer tjenester eller setter ut arbeidsoppgaver og/eller funksjoner til eksterne leverandører. Det kan for eksempel være at kommunen anskaffer et fagsystem eller digital lagringsløsning i form av skytjeneste, setter ut drift av IKT-tjenester til ekstern leverandør, kommunesamarbeid, eller setter ut driften av en kommunal tjeneste i sin helhet.

Ved tjenesteutsetting kan ansvaret for hele eller deler av oppgaven settes bort, men risikoen det medfører og ansvaret for å etterleve lovverk og krav kan aldri settes bort.

Hvis tjenesteutsettingen involverer håndtering av kommunens informasjonsverdier, eier fortsatt kommunen all risiko knyttet til informasjonsbehandlingen. Kommunedirektøren er derfor ansvarlig for at informasjonssikkerhet og personvern ivaretas uansett om tjenesten driftes i sin helhet av kommunen, eller om den helt eller delvis utføres av eksterne leverandører. Kommunedirektøren har også ansvaret der tjenester anskaffes eller driftes i et kommunalt IKT-samarbeid, selv om noen andre utfører oppgaven i det daglige.

Informasjonssikkerhet og personvern ved tjenesteutsetting må ivaretas i hele tjenestens eksisterer, fra planlegging til avvikling. Dette gjøres ved å foreta risikovurderinger, stille krav til leverandørene i anskaffelsen, gjennomføre kontrolltiltak og revisjoner underveis i avtaleforholdet og avtalefeste hva som gjøres med informasjonsverdiene ved avtalens slutt.

Ved tjenesteutsetting hvor anskaffelsen ikke involverer bruk av en konkret digital tjeneste, for eksempel ved kjøp av konsulenttjenester eller innovative anskaffelser, skal det også stilles krav til leverandørens styring av informasjonssikkerhet og personvern. I slike tilfeller er det viktig å sikre at leverandøren har et styringssystem og tilstrekkelig kompetanse på fagområdet.

Typiske risikoer ved tjenesteutsetting:

- mangelfulle eller manglende risikovurderinger av informasjonssikkerhet og personvern
- mangelfull kartlegging og verdivurdering av på kommunens informasjonsverdier
- leverandøravtaler kontraktfester ikke hvilket sikkerhetsnivå som skal ligge i leveransen
- manglende eller mangelfulle databehandleravtaler og dokumentasjon i form av behandlingsprotokoller
- kommunen har ikke tilstrekkelig kompetanse for stille krav til leverandører eller sørge for god forvaltning av tjenesten i avtaleperioden
- manglende oversikt over leverandører og deres underleverandører (leverandørkjeden)
- manglende oversikt over hvilke avhengigheter kommunen har i leverandør- og verdikjeder (hendelser hos leverandøren som kan få konsekvenser for kommunen)
- manglende reell innsikt i leverandørens tiltak og rutiner

Kommunal sektor tjenestestytter ofte funksjoner og arbeidsoppgaver av økonomiske eller praktiske årsaker, eller fordi de ikke har kompetanse eller personell for å drifte den selv. Kommunen må likevel sørge for å ha nødvendig kompetanse og ressurser for å kunne håndtere risikoene og følge opp leverandørene.



Det er ikke mulig å sette ut ansvaret for personvern og informasjonssikkerhet. Det ligger alltid hos kommunedirektøren.

SJEKKLISTE FOR TJENESTEUTSETTING

Sjekkliste for tjenesteutsetting		Ja	Vet ikke	Nei
1	Har kommunen gjennomført nødvendig vurderinger, herunder risikovurdering, av om tjenesteutsettinger kan gjennomføres og hvordan?			
2	Omfatter risikovurderingene både personvern og informasjonssikkerhet?			
3	Har kommunen sikret tilstrekkelig personvern og informasjonssikkerhet i kontrakten som regulerer tjenesteutsettingen, og er ansvarsforholdet tydelig?			
4	Har kommunen regulert hvordan den skal gjøre god forvaltning, ved blant annet å følge opp leverandører og leveranser, gjennomføre revisjoner samt ivareta kommunens endringsbehov i kontrakten?			
5	Har kommunen regulert forholdet om hvordan tilbakeføring og sletting skal skje ved opphør av tjenesteutsettingen?			
6	Følger kommunen opp sine eksterne leverandører gjennom sikkerhetsrevisjoner?			
7	Har kommunen tilstrekkelige ressurser og kompetanse til å følge opp tjenesteutsettingen? - Dette innebærer virksomhetskompetanse, kompetanse om informasjonssikkerhet, personvern og risikostyring, integrasjonskompetanse, kompetanse om anskaffelser og juridisk kompetanse.			
8	Revideres risikovurderinger for tjenesteutsetting jevnlig?			
9	Har kommunen inngått avtale om behandling av personopplysninger med leverandøren (databehandlertavtale)?			
10	Har kommunen inngått sikkerhetsavtale i henhold til sikkerhetsloven der det er nødvendig?			
11	Er behandlingsprotokollen oppdatert med at tjenesten er satt ut?			
12	Er det gjennomført personvernkonsekvensvurderinger der dette er nødvendig?			
13	Har kommunen oversikt over hvor personopplysninger lagres. I EØS eller utenfor EØS?			
14	I tilfeller hvor personopplysninger lagres utenfor EØS, har kommunen iverksatt tiltak for å sikre personvernet og inngått tilstrekkelige avtaler (gyldig overføringsgrunnlag)?			
15	Har kommunen oversikt over hvem hos leverandøren som har tilgang til informasjonen?			
16	Har kommunen stilt krav til leverandørens styringssystem for informasjonssikkerhet i tillegg til tekniske og organisatoriske tiltak?			
17	Har kommunen sikret at taushetsplikten ivaretas i tjenesteutsettingen?			
18	Ivaretar kommunen ansvaret for informasjonssikkerhet og personvern for tjenester som driftes i eventuelle IKT-samarbeid?			



Tenk gjennom

- Har vi oversikt over alle IT-tjenestene og applikasjonene vi bruker i kommunen?
- Har vi oversikt over om våre leverandører etterlever krav til personvern og informasjonssikkerhet?
- Har vi tilstrekkelig kompetanse for å håndtere risikoene ved tjenesteutsetting?