

Hvorfor kommunen bør bruke datasikkerhetsavtale

Kommunen bør bruke datasikkerhetsavtale for å sikre at digitale løsninger og leverandører ikke hindrer levering av kommunale tjenester. Avtalen er et styringsverktøy som tydeliggjør krav til digital sikkerhet, drift og beredskap hos leverandører som tjenestene er avhengige av.

Datasikkerhetsavtalen brukes når en leverandør leverer eller drifter systemer, plattformer eller tjenester som er viktige eller kritiske for kommunens virksomhet, for eksempel fagsystemer, integrasjoner, skyløsninger, driftstjenester eller velferdsteknologi. Dette gjelder uavhengig av om leverandøren behandler personopplysninger.

En databehandleravtale regulerer kun behandling av personopplysninger etter personvernregelverket. Den sier ingenting om tilgjengelighet, beredskap, gjenoppretting, hendelseshåndtering eller leveransesikkerhet. Mange leverandører som er avgjørende for tjenesteleveransen er heller ikke databehandlere i juridisk forstand, men tekniske eller driftsmessige tjenesteleverandører.

Digitalsikkerhetsloven stiller krav til at kommunen har kontroll på digitale risikoer og avhengigheter i leverandørkjeden. Disse kravene kan ikke ivaretas gjennom databehandleravtaler alene, men må reguleres gjennom egne kontraktsbestemmelser.

Datasikkerhetsavtalen:

- sikrer tydelige krav til drift, sikkerhet og beredskap
- gir kommunen bedre styring og forutsigbarhet
- understøtter forsvarlig tjenesteleveranse og etterlevelse av lovkrav

Der både personvern og leveransesikkerhet er relevant, brukes datasikkerhetsavtale og databehandleravtale side om side. Databehandleravtalen erstatter aldri datasikkerhetsavtalen.

Hva er en datasikkerhetsavtale – kort forklart

En datasikkerhetsavtale er en avtale som:

- regulerer krav til digital sikkerhet og leveransesikkerhet
- uavhengig av om leverandøren behandler personopplysninger eller ikke
- og dekker:
 - tilgjengelighet
 - integritet
 - konfidensialitet
 - robusthet

- varsling og håndtering av hendelser
- beredskap og gjenoppretting
- innsikt i verdikjeden

Den er forankret i:

- NSMs grunnprinsipper, kommunens informasjonssikkerhetspolicy, digitalsikkerhetsloven og NIS2
- kommunens ansvar for forsvarlig tjenesteleveranse
- og i praksis: drifts- og beredskapsansvar

Hvorfor bruke en datasikkerhetsavtale?

En datasikkerhetsavtale brukes for å regulere krav til digital sikkerhet når en leverandør får tilgang til eller drifter kommunens systemer eller data, uavhengig av om det behandles personopplysninger.

Formålet er å sikre at leverandøren opprettholder et forsvarlig nivå av digital sikkerhet i tråd med kravene i Lov om digital sikkerhet.

Dette innebærer blant annet krav til:

- risikostyring
- tekniske og organisatoriske sikkerhetstiltak
- håndtering av sikkerhetshendelser
- beredskap og kontinuitet
- leverandørstyring.

Datasikkerhetsavtalen regulerer derfor sikkerheten i systemene og tjenestene, ikke bare behandlingen av personopplysninger.

Hvordan de to avtalene kan eksistere side om side

Situasjon	Riktig avtale
Kun teknisk leveranse	Datasikkerhetsavtale
Personopplysninger behandles	Databehandleravtale
Kritisk tjeneste + personopplysninger	Begge
Leverandør kun infrastruktur	Datasikkerhetsavtale

Databehandleravtale erstatter **aldri** datasikkerhetsavtale.