Anskaffelser - hvordan sikre at behov og lovkrav til personvern og informasjonssikkerhet blir ivaretatt

Foredragsholdere

22.10.23

Informasjonssikkerhet og personvern – sett fra mange leverandører og innkjøpere ståsted

Alt for komplisert

Alt for strenge krav

Usikkerhet hva som gjelder for «oss»

Hjelp… for noe kjedelig opplegg

Det er jo sånn lover og greier, det får noen andre ta seg av

Typiske krav som stilles i forbindelse med anskaffelser

- Normen skal følges
- Leverandøren skal følge Normen
- Normens samlete krav skal besvares (294 stk.)
- Leverandøren skal ha et styringssystem for Informasjonssikkerhet og personvern
- Oppdragsgivers fjernaksessløsning SKAL benyttes

- «Løsningen må være egnet til å ivareta relevante krav som stilles i den til enhver tid gjeldende Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen).»

Ansvar for å følge kravene i Normen

Den som er ansvarlig etter lovgivning for behandling av personopplysninger (dataansvarlig/behandlingsansvarlig) har ansvaret for at krav til informasjonssikkerhet og personvern følges gjennom hele leveransekjeden.

I leveranser av f.eks. tjenester, maskinvare eller systemer skal det avtales skriftlig med leverandører hvilke sikkerhetskrav som skal oppfylles for at den dataansvarlige skal kunne oppfylle sitt ansvar.

Hvilke av Normens krav som gjennom avtale gjelder for leverandører, er avhengig av hva slags type leveranse det er snakk om, for eksempel:

- Databehandling, i form av for eksempel bruk skytjenester eller driftstjenester for å behandle helse- og personopplysninger på vegne av dataansvarlig
- Vedlikehold, for eksempel ved fysisk service eller fjernaksess
- Leveranse av løsninger og systemer

Ivaretakelse av lovkrav generelt i anskaffelser for helsesektor

Veileder for Informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren

- Veilederen beskriver tiltak og forventninger til IKT-løsninger, medisinsk utstyr og operasjonell teknologi (OT) fra leverandørens perspektiv.

- Referansegruppe bestående av:
  - IT-leverandør til sektoren
  - Flere leverandører av Medisinsk utstyr
  - Driftsorganisasjoner innen spesialist (IT og med-tek)
  - Sykehusinnkjøp og Norsk helsenett
  - Innkjøpskompetanse i kommune

NORMEN

Kravene

Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren Versjon 6.1					
Krav.nr	Overordnede kapittel i Normen	Kap. i Normen	Kravbeskrivelse	Tekst for bruk i kravspesifikasjon - Leverandøren er databehandler	T I (
077.	C. Grunnleggende om behandling av helse- og personopplysninger	4.2.3 Innsyn (Plikter og krav ved behandling av helse- og personopplysninger)	Virksomheten skal sikre at den registrerte kan få innsyn i egen logg over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt.	Tilbuder skal sikre at pasieter og brukere som blir registert i systemet kan få innsyn i hvem og virksomhetsilknytning til den som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt. Det bør legges til rette for at oppdragsiver skal kunne adminsiterer og hente ut innsynslogger uten å måtte involvere tilbyder.	

Kravbeskrivelse	Tekst for bruk i kravspesifikasjon - Leverandøren er databehandler
Virksomheten skal sikre at den registrerte kan få innsyn i egen logg over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt.	Tilbuder skal sikre at pasieter og brukere som blir registert i systemet kan få innsyn i hvem og virksomhetsilknytning til den som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt. Det bør legges til rette for at oppdragsiver skal kunne adminsiterer og hente ut innsynslogger uten å måtte involvere tilbyder.