

Administrationens faktuelle bemærkninger til drøftelse i FU vedr. cybersikkerhed og medicoteknisk udstyr

Medlemsforslaget lægger op til at Forretningsudvalget:

- 1. drøfter, hvordan Region Hovedstaden forholder sig til truslen fra bagdøre i medicoteknisk udstyr,*
- 2. orienteres, om Region Hovedstadens brug af medicoteknisk udstyr fra lande, hvor der kan være sikkerhedsmæssige udfordringer ift. håndtering af data, herunder fra Kina – samt om overvejelserne herom og*
- 3. drøfter, hvordan Region Hovedstadens indkøbspolitikker kan skærpes, så der tages højde for Center for Cybersikkerheds vurdering af trusselsbilledet mod sundhedssektoren.*

Herunder følger administrationens samlede bemærkninger:

Ad 1)

Region Hovedstaden følger løbende myndighedernes trusselsvurderinger inden for cyber- og informationssikkerhedsområdet. Det gælder både vurderinger fra Center for Cybersikkerhed, Politiets Efterretningstjeneste og Forsvarets Efterretningstjeneste. Hertil modtager Region Hovedstaden varsler fra både Center for Cybersikkerhed og den decentrale cyber- og informationssikkerhedsenhed i sundhedssektoren (DCISSund), når der identificeres sårbarheder i systemer eller udstyr, som kan udnyttes af hackere – herunder sårbarheder i medicoteknisk udstyr.

Med udgangspunkt i myndighedernes anbefalinger foretager Region Hovedstaden en konkret risikovurdering af det pågældende medicotekniske udstyr for dels at sikre regionens generelle cyber- og informationssikkerhed, og dels at det pågældende medicotekniske udstyr ikke påvirker patientsikkerheden.

Hertil har Region Hovedstaden en række generelle og supplerende retningslinjer for informationssikkerhed og databeskyttelse, der skal imødegå det trusselsbillede, som regionen står overfor. Dette indebærer blandt andet regionens retningslinje for videoovervågning, som blev godkendt af koncernledelsen i februar 2024 og udmønter Center for Cybersikkerheds anbefalinger vedrørende anvendelse af overvågningskameraer.

Som en del af Region Hovedstadens strategi for cyber- og informationssikkerhed 2024-2027 er etableret et initiativ vedrørende øget kontrol med Internet of Things (IoT), der blandt andet skal øge sikkerheden i medicoteknisk udstyr ved at overvåge eventuelle sårbarheder i udstyret.

Region Hovedstadens retningslinjer og arbejde med cyber- og informationssikkerhed tager således udgangspunkt i konkrete anbefalinger eller varslers om bagdøre i medicoteknisk udstyr, og regionen træffer sikkerhedsmæssige foranstaltninger på baggrund heraf for at minimere risikoen for konsekvenser på patientsikkerheden.

Region Hovedstadens medicotekniske udstyr har i gennemsnit en høj alder, hvilket alt andet lige giver en usikkerhed. Blandt andet på den baggrund arbejdes der på at afsætte flere penge til apparatur i Budget 2026 med henblik på løbende at få sikret medicoteknisk udstyr til de opdaterede krav.

Ad 2)

Region Hovedstaden udelukker ikke brug af medicoteknisk udstyr fra kinesiske producenter med mindre, at der foreligger et konkret varsel fra nationale myndigheder jf. ovenstående. Alt regionens medicotekniske udstyr håndteres efter regionens standard procedurer ift. sikkerhed, hvor der altid bliver indgået en databehandleraftale ligesom det kontrolleres, hvorvidt udstyret har de nødvendige certificeringer ift. MDR eller IVDR.

I forhold til medicoteknisk udstyr fra Kina er regionens selvstændige handlerum begrænset. Regionen agerer altid i overensstemmelse med de til enhver tid gældende nationale retningslinjer.

Ad 3)

Indkøb af medicoteknisk udstyr beror på en konkret vurdering af de sikkerhedsrisici, som udstyret vil kunne medføre og er ikke udelukkende fokuseret omkring det land, som udstyret stammer fra. Herudover kan det nævnes, at Region Hovedstaden er i gang med at udarbejde en række sikkerhedsmæssige basiskrav for indkøb i regionen, der også vil omfatte indkøb af medicoteknisk udstyr. Regionen er ligeledes i dialog med leverandørerne af medicoteknisk udstyr med henblik på at skærpe det sikkerhedsmæssige fokus i forbindelse med produktion af udstyret.

Regionen er underlagt de udbudsretlige regler ved indkøb af medicoteknisk udstyr, hvilket blandt andet indebærer at de krav vi stiller til medicoteknisk udstyr som udgangspunkt skal give økonomiske aktører lige adgang til udbuddet, og ikke må medføre, at der skabes ubegrundede hindringer for, at udbuddet åbnes for konkurrence, ligesom at regionens krav skal være i overensstemmelse med ligebehandlings-, gennemsigtigheds- og proportionalitetsprincippet. Det kan i den forbindelse ikke afvises, at hensynet til cybersikkerhed kan udgøre en saglig begrundelse for at vi stiller krav, der begrænser konkurrencen, men vurderingen deraf skal i henhold til udbudsreglerne foretages konkret for anskaffelsen/ udbuddet.

Udbudsreglerne begrænser regionens mulighed for i udbud at forfølge et formål om at udelukke økonomiske aktører fra konkurrencen baseret på deres etableringsland, men der kan konkret ske udelukkelse af en aktør, hvis denne er omfattet af én eller flere udelukkelsesgrunde i udbudsloven, og aktøren ikke kan dokumentere selfcleaning. Regionen anvender som udgangspunkt alle udbudslovens udelukkelsesgrunde i udbud, dog er der ingen udelukkelsesgrund, der specifikt angår forhold så som cybersikkerhed.

Derudover er der med Investeringscreeningsloven indført regler gældende for særlige økonomiske aftaler, der skal indgås med virksomheder, der er etableret i lande udenfor EU eller EFTA eller er kontrolleret af personer eller virksomheder fra lande udenfor EU eller EFTA. For sådanne aftaler gælder, at vindende tilbudsgiver skal anmode Erhvervsstyrelsen om tilladelse til at indgå kontrakten med regionen. Formålet med loven er at forhindre, at en aftale med sådan en leverandør vil kunne udgøre en trussel mod den nationale sikkerhed eller offentlige orden i Danmark. Investeringscreeningsloven finder fx aktuel anvendelse ved udbud af telefoniysdelser, hvor vindende tilbudsgiver vil skulle opnå tilladelse fra Erhvervsstyrelsen, hvis denne er kontrolleret (bestemmende indflydelse) udenfor EU eller EFTA. Dette kunne ligeledes finde anvendelse ved fx medicoteknisk udstyr.