Klagenævnet for Udbud
(Jakob O. Ebbensgaard, Maria Haugaard)

J.nr.: 22/17491
10. maj 2023

K E N D E L S E

Filial af Trend Micro Emea Limited
(advokat Thomas Grønkær, København)

mod

Region Hovedstaden
(advokat Tom Holsøe og erhvervsjuridisk rådgiver Emil Bisgaard, København)

Sagen angår Region Hovedstadens indkøb af endpoint-beskyttelsessoftware i henhold til SKI's dynamiske indkøbssystem 02.06 "Standardsoftware", som blev udbudt ved udbudsbekendtgørelse nr. 2020/S 220-539774, og som trådte i kraft den 28. marts 2021.

Region Hovedstaden, der er kunde hos SKI og tilsluttet SKI's dynamiske indkøbssystem 02.06, udsendte den 15. november 2022 en opfordringsskrivelse med tilbudsfrist den 28. november 2022 til leverandører på det dynamiske indkøbssystem 02.06 om levering af endpoint-, cloudbeskyttelses- og SOAR-software til regionen.

Den 22. november 2022 rettede Trend Micro henvendelse til Region Hovedstaden og gjorde opmærksom på, at Trend Micro ikke så sig i stand til at afgive et tilbud på levering af endpoint-, cloudbeskyttelses- og SOAR-software grundet de tekniske mindstekrav, der var stillet.

Den 2. december 2022 besluttede Region Hovedstaden at indgå kontrakt med Conscia Danmark A/S, og kontrakt blev herefter indgået den 14. december 2022.

Den 28. december 2022 indgav Trend Micro klage til Klagenævnet for Udbud over Region Hovedstaden. Klagen har været behandlet skriftligt.

Trend Micro har nedlagt følgende påstande:

Påstand 1
Klagenævnet for Udbud skal konstatere, at Region Hovedstaden har handlet i strid med udbudslovens § 40, stk. 4, samt de grundlæggende principper om ligebehandling og proportionalitet i udbudslovens § 2 i forbindelse med udbuddet af en kontrakt om levering af endpoint-, cloudbeskyttelse og SOAR, idet Region Hovedstaden har fastsat tekniske specifikationer, som ikke er sagligt begrundede og proportionale med kontraktens værdi og mål, og som derfor medfører en kunstig indsnævring af konkurrencen.

Påstand 2
Klagenævnet for Udbud skal annullere Region Hovedstadens beslutning af 2. december 2022 om at tildele kontrakten om levering af endpoint-, cloudbeskyttelse og SOAR til Conscia Danmark A/S.

Påstand 3
Klagenævnet for Udbud skal erklære Region Hovedstadens kontrakt med Conscia Danmark A/S om levering af endpoint-, cloudbeskyttelse og SOAR for uden virkning i medfør af § 17, stk. 1, nr. 4, i lov om Klagenævnet for Udbud.

Påstand 4
Klagenævnet for Udbud skal pålægge Region Hovedstaden en alternativ sanktion, jf. § 18, stk. 2, nr. 3, i lov om Klagenævnet for Udbud.

Trend Micro har tilkendegivet senere at ville nedlægge påstand om erstatning.

Region Hovedstaden har nedlagt påstand om, at klagen ikke tages til følge.

Klagenævnet har den 2. januar 2023 meddelt Region Hovedstadens kontraktpart, Conscia Danmark A/S, at det er muligt at intervenere i sagen, jf. lov om Klagenævnet for Udbud § 6, stk. 5.

Conscia Danmark A/S har ikke besvaret klagenævnets henvendelse.

Sagens nærmere omstændigheder

Af udbudsbekendtgørelsen og udbudsbetingelserne for det dynamiske indkøbssystem SKI 02.06 fremgår bl.a., at SKI 02.06 omfatter standardsoftware, defineret som software, der er præfabrikeret og kommercielt tilgængeligt, og relaterede ydelser.

Af kundevejledningen til SKI 02.06 fremgår bl.a.:

> "Bilag 1 - Kundens opgavebeskrivelse
>
> Her beskriver du dit indkøbsbehov så præcist, at en tilbudsgiver kan vurdere dit indkøbsbehov. Vær opmærksom på, at du jf. udbudsloven ikke må efterspørge en navngiven licens/en navngiven producent. Du må dog gerne beskrive dit nuværende it-miljø, herunder detaljer om dine nuværende licenser."

Den 15. november 2022 udsendte Region Hovedstaden en opfordringsskrivelse til leverandørerne på SKI 02.06 om levering af endpoint-, cloudbeskyttelses- og SOAR-software til regionen.

Af opfordringsskrivelsen fremgår, at regionen ønskede at "anskaffe licenser til endpoint-, cloudbeskyttelse og SOAR samt tilknyttede ydelser med henblik på øget sikkerhed af Kundens infrastruktur". Regionen havde i den forbindelse opgjort et behov for at anskaffe licenser til regionens 52.000 endpoints (PC-klienter) og 60.000 cloudbrugere med en varighed fra den 1. januar 2023 til den 29. juli 2025.

Tildelingskriteriet var "bedste forhold mellem pris og kvalitet". Af opfordringsskrivelsens pkt. 7 fremgår følgende om konditionsmæssighed:

”Tilbuddet må ikke indeholde forbehold over for Mindstekrav eller grundlæggende elementer i udbudsmaterialet. Forbehold over for Mindstekrav eller grundlæggende elementer i udbudsmaterialet medfører, at tilbuddet bliver afvist.

Ved afgivelsen af tilbuddet skal tilbudsgiverne tillige opfylde alle Krav. Tilbud, der indeholder forbehold over for Krav, vil blive afvist som ukonditionsmæssige, hvis forbeholdet vedrører grundlæggende elementer i udbuddet. Ved grundlæggende elementer forstås forhold der indebærer, at konkurrencen fordrejes i betydeligt omfang, hvis der tages forbehold. Flere forbehold over for ikke grundlæggende elementer kan samlet set udgøre forbehold over for grundlæggende elementer.”

Af Leverandørens løsningsbeskrivelse fremgår bl.a.:

”Det tillægges positiv betydning i hvilket omfang Standardsoftwarens anvendelse af firewallgenererede logdata fra Kundens eksisterende firewalls, jf. punkt 3.3, understøtter tidlig og korrekt detektion af sikkerhedshændelser baseret på netværkstrafikken.”

Af bilaget Kundens opgavebeskrivelse fremgår bl.a.:

”2.1.1 Supplerende specifikation

Kunden ønsker at købe Standardsoftware til beskyttelse af endpoints (PCklienter) og cloudbrugere jf. pkt. 3.1 (Eksisterende it-miljø).

MK1: Leverandøren skal levere licenser til Standardsoftware jf. pkt. 2.1.1.1 (Endpointbeskyttelse), 2.1.1.2 (Cloudbeskyttelse) og 2.1.1.3 (SOAR).

2.1.1.1 Endpointbeskyttelse

…

2.1.1.1.2 Anvendelse af firewallgenererede logs

K12: Standardsoftwaren skal kunne hente og anvende firewallgenererede logdata fra Kundens eksisterende firewalls, jf. punkt 3.1 (Eksisterende infrastruktur), indeholdende informationer om HTTP user agent, automatisk IP-tildeling via DHCP og DNS-opslag herunder med det formål, at Kunden kan benytte de eksisterende firewalls, jf. punkt 3.1 (Eksisterende infrastruktur), som sensorer i forhold til analyse af netværkstrafikken.

…

2.1.1.1.4 Integration med Kundens sandkasse-løsning.

K18: Standardsoftwaren skal integrere til og benytte Kundens sandkasse-løsning, jf. punkt 3.1 (Eksisterende infrastruktur), således at ukendte filer analyseres via netværket. Med ukendt menes, at Kundens sandkasseløsning ikke har kategoriseret filen som ”benign”, ”suspicious” eller ”malware”.

K19: Standardsoftwaren skal sende alle ukendte “Portable executable files” til Kundens sandkasse-løsning, jf. punkt 3.1 (Eksisterende infrastruktur).

…

3 Eksisterende it-miljø

I nærværende punkt beskrives Kundens it-miljø.

Beskrivelsen understøtter Leverandørens opfyldelse af Leveringskontrakten. Beskrivelsen af Kundens it-miljø indeholder ingen selvstændig kravsætning til Leverandøren.

Ved underskrift af Leveringskontrakten beskrives Kundens it-miljø, således som det eksisterer forud for kontraktindgåelsen.

3.1 Eksisterende infrastruktur

Kunden benytter i dag:

- Firewalls:
  - 90 stk. Palo Alto Networks Next Generation Firewalls (NGFW) som er på version 9.1.x af PAN-OS, der er softwaren, som benyttes på alle Kundens firewalls.
- Sandkasse-løsning:
  - Palo Alto Networks Wildfire sandbox
- Cortex XDR Pro
- Microsoft Azure
- VMWare
- Amazon Web Services
- Trend Micro (Apex One, Officescan, Deep Security, Cloud App Security)
- Citrix
- Endpoints (Servere) 7.000 stk. fordelt på:
  - Fysiske og virtuelle Windows servere (alle versioner fra 2003, både 32-bit og 64-bit versioner)

    - Fysiske og virtuelle Linux (Oracle Linux, RedHat og Ubuntu)
- Endpoints (PCklienter) 52.000 fordelt på:
    - Fysiske og virtuelle computere (Windows XP, Windows 7, Windows 10 og Windows 11)
    - Fysiske og virtuelle Linux computere (Oracle Linux, Redhat og Ubuntu)
- Cloudbrugere:
    - 60.000 stk."

Forud for det konkrete udbud, som sagen angår, havde Region Hovedstaden den 26. juli 2022 iværksat et lignende udbud under det samme dynamiske indkøbssystem vedrørende 7.000 licenser til endpoint-beskyttelse. I forbindelse med det tidligere udbud kontaktede Trend Micro Region Hovedstaden ved e-mail af 4. juli 2022 og anførte, at virksomheden ikke så sig i stand til at afgive tilbud. Om baggrunden herfor anførte Trend Micro:

> "Baggrunden herfor er, at der er en række krav i bilaget "Kundens opgavebeskrivelse", som stiller krav om, at den tilbudte software kan integrere med Region Hovedstadens eksisterende it-infrastruktur, som er baseret på produkter fra Palo Alto:
>
> - Krav 12, kan kun leveres af Palo Alto og der henvises specifikt til integration med Region Hovedstadens "Palo Alto firewall".
> - Krav 18, som vedrører integration inden at den tilbudte løsning rammer End-pointet. Dette krav kan kun løses med en "Palo Alto agent", idet der skal benyttes Palo Alto netværks appliances som afsender af kategoriseringen. På den baggrund vil sikkerhedsleverandører i Endpoint protection-branchen ikke kunne opfylde dette krav uden levering af Palo Alto produkter.
> - Krav 19, det fremgår specifikt at der skal kommunikeres via kundens Firewall sandbox løsning (som er Palo Alto), automatisk, og det kan kun Palo Alto levere når det kommer til udbuddets område som er Endpoint protection
>
> Efter min klients opfattelse er det således ikke muligt for andre end Palo Alto at tilbyde denne integration, hvorfor det er udelukket for andre end Palo Alto at byde på det pågældende mini-udbud."

Trend Micro opfordrede Region Hovedstaden til at frafalde de pågældende krav, således at det var muligt for andre virksomheder med konkurrerende produkter at levere det krævede software til regionen.

Ved e-mail af 8. juli 2022 til Trend Micro anførte Region Hovedstaden, at der efter regionens opfattelse ikke var grundlag for at frafalde de pågældende krav.

Region Hovedstaden modtog tilbud på de 7.000 endpoint-licenser fra Atea A/S og Conscia Danmark A/S. Tilbuddene indeholdt alene produkter af fabrikatet "Palo Alto". Den 15. august 2022 tildelte Region Hovedstaden kontrakten til Conscia Danmark A/S.

Trend Micro har klaget over dette udbud til Klagenævnet for Udbud. Klagenævnet har behandlet sagen under sag nr. 22/14579, og har den 22. marts 2023 afsagt kendelse om, at klagen ikke tages til følge.

I den foreliggende klagesag rettede Trend Micro henvendelse til Region Hovedstaden ved e-mail af 22. november 2022. I e-mailen gjorde Trend Micro opmærksom på, at virksomheden heller ikke i dette udbud så sig i stand til at levere et tilbud på levering af endpoint-, cloudbeskyttelses- og SOAR-software grundet de tekniske mindstekrav. Regionen afviste ligeledes i dette udbud at ændre kravene.

Ved tilbudsfristens udløb den 28. november 2022 havde regionen modtaget tilbud fra henholdsvis Atea A/S og Conscia Danmark A/S. Conscia Danmark A/S bød ind med endpoint-, cloudbeskyttelses- og SOAR-software fra producenten Palo Alto, mens Atea A/S bød ind med software fra producenten Microsoft.

Region Hovedstaden har oplyst, at regionen ikke har foretaget en nærmere undersøgelse af, om Atea A/S' tilbudte produkt lever op til kravene i opgavebeskrivelsen, idet regionen ikke er forpligtet hertil, jf. udbudslovens § 159. Atea A/S anfører i tilbuddet, at "Atea og Microsoft imødekommer de stillede krav ved hjælp af …". Regionen har lagt til grund, at Atea A/S' tilbud levede op til de stillede krav. Da tilbuddet fra Conscia Danmark A/S blev vurderet at have det bedste forhold mellem pris og kvalitet, har regionen ikke foretaget nærmere undersøgelser af tilbuddet fra Atea A/S.

Kontrakten blev tildelt Conscia Danmark A/S den 2. december 2022.

Den 14. december 2022 blev kontrakten underskrevet.

Region Hovedstaden har for klagenævnet fremlagt en analyse fra 2021 af regionens informationssikkerhed. Analysen er udført efter CIS20-standarden. Af analysen fremgår bl.a.:

> ”Der er generelt etableret et godt overblik over Regionens knudepunkter imod internettet, og alle internetvendte tjenester er beskyttede af Palo Alto firewalls, hvor der er URL filtrering, og der blokeres på 8 kategorier af ondsindede hjemmesider, ud fra et sikkerhedsmæssigt hensyn. Identifikationen af ondsindede hjemmesider er dog en manuel proces og der findes grænsetilfælde, hvor der ikke er kendskab til, om der gennemføres blokering, hvis det ikke er netværksafdelingen, som administrerer udstyret.
>
> Der gennemføres monitorering af netværksforbindelser via Palo Alto, men der er ikke noget overblik over, hvilke netværksforbindelser der er autoriseret, så det er ikke muligt at identificere hvilke, som ikke er autoriseret.
> …
> Der anvendes generelt intrution prevention på alle Palo Alto bokse, dog er det blevet oplyst, at der er usikkerhed omkring, hvor dækkende det nuværende setup er.”

Region Hovedstaden har oplyst, at regionen af sikkerhedsmæssige, organisatoriske, tekniske og økonomiske grunde har ønsket at bevare sin eksisterende it-infrastruktur, herunder eksisterende firewalls og sandkasseløsning. Baggrunden for dette er ifølge regionen, at det vil indebære en betydelig meromkostning, hvis regionen skal udskifte alle sine firewalls, ligesom der også ville være en vis teknisk og organisatorisk risiko forbundet med omstillingen. Den tekniske risiko består bl.a. i, hvorledes en udskiftning vil passe ind i regionens arkitektur og opsætning, hvor opsætning af firewalls er en ret kompleks opgave. Dertil kommer, at en udskiftning af regionens firewalls – ud over omkostningerne til anskaffelsen – bl.a. ville afstedkomme et behov for opdatering af firewall-regler, politikker og vejledninger, hvilket vil være ressourcekrævende og udgøre en meromkostning. Herudover er det ifølge regionen generelt anerkendt, at it-projekter er forbundet med risici, herunder forretningsmæssige, tekniske og økonomiske risici.

Region Hovedstaden har henvist til Danske Regioners fælles målsætning fra marts 2021, hvor bestyrelsen har udstukket den strategiske retning i forhold til regionernes arbejde med cyber- og informationssikkerhed med ønske om at opnå et fælles ambitionsniveau på CIS20-modenhedsskalaen.

Region Hovedstaden har til belysning af hensigtsmæssigheden i at sikre, at endpoint-beskyttelse kan samarbejde med firewalls, fremlagt et eksempel fra SentinelOne: "Why you need endpoint protection and firewalls working together for true security", hvoraf fremgår bl.a.:

> "To protect against these increasingly sophisticated threats, organisations must take an interconnected, holistic approach to security. One of the most effective strategies is to combine technologies that can identify threats across the enterprise network and act to prevent them in concert before they can spread. Integrating a firewall solution with an next-gen protection platform, including integrated Endpoint Detection and Response (EDR) capabilities, allows the two solutions to work together and provide complete, integrated security."

Endelig har regionen oplyst, at antallet af firewalls bl.a. hænger sammen med antallet af fysiske lokationer, mens antallet af endpoint-licenser hænger sammen med de omfattede antal endpoints (PC-klient og cloudbrugere). Antallet af endpoint-licenser er derfor ikke knyttet til antallet af firewall-licenser.

Parternes anbringender

Ad påstand 1

Trend Micro har gjort gældende, at det følger af udbudslovens § 40, stk. 4, at de tekniske specifikationer skal give økonomiske aktører lige adgang til udbuddet og ikke må bevirke, at der skabes ubegrundede hindringer for, at et udbud åbnes for konkurrence. Bestemmelsen skal sikre, at ordregiver ikke i de tekniske specifikationer skaber ubegrundede hindringer for konkurrencen eller på andre måder kunstigt indsnævrer konkurrencen. Bestemmelsen er et udtryk for ligebehandlingsprincippet i udbudslovens § 2 og fastsætter krav om, at ordregiver skal kunne anføre saglige grunde til at stille krav til tekniske specifikationer, som har en konkurrencebegrænsende virkning. En ordregiver, der vælger at fastsætte tekniske specifikationer i strid med ordlyden af § 40, stk. 4, må kunne dokumentere, og bærer bevisbyrden for, at kravene i opgavebeskrivelsen er sagligt begrundede. En ordregiver kan som udgangspunkt fastsætte tekniske specifikationer, som er passende og nødvendige, og som er forbundet med kontraktens genstand. Dette kræver dog, at kravene er sagligt begrundede og ikke mindst proportionale.

Regionen har fastlagt en række krav, som indebærer en uretmæssig indskrænkning af konkurrencen til kun at kunne omfatte Palo Alto-produkter. Sådanne detaljerede krav kan alene løses af bestemte produkter, og kravene har dermed en konkurrencebegrænsende virkning. Det har ikke været muligt at finde andet kendt endpoint- og cloudbeskyttelsessoftware end produkter fra Palo Alto, der opfylder de specifikke krav, som Region Hovedstaden har opstillet.

Kravene forhindrer effektivt, at leverandører af endpoint- og cloudbeskyttelse af andre fabrikater end Palo Alto kan afgive et konditionsmæssigt tilbud.

I medfør af opgavebeskrivelsens krav 12 skulle endpoint-licenserne være i stand til at hente og anvende firewallgenererede logdata fra regionens eksisterende firewalls (Palo Alto Networks Next Generation Firewalls, jf. opgaveskrivelsens pkt. 3.1). Selvom regionen i øjeblikket kun har 90 stk. Palo Alto firewall-licenser, omfattede indkøbet 52.000 endpoint (PC-klient) licenser og 60.000 cloudbrugere. Herudover har regionen anskaffet yderligere 7.000 endpoint licenser med samme krav.

På trods af det meget beskedne antal firewall-licenser (90 stk.) i forhold til endpoint-licenser mv. giver regionen ikke mulighed for, at leverandører f.eks. også tilbyder alternative firewall-licenser som en del af tilbuddet eller ved at tillægge skifteomkostninger.

Regionen har dermed ikke gjort forsøg på at minimere den konkurrencebegrænsende virkning af de opstillede krav på nogen måde. Krav K12, K18 og K19 bevirker, at kun Palo Alto-produkter kan opfylde regionens behov, og giver ikke plads til, at andre konkurrerende producenter kan tilbyde samme overordnede løsninger og funktionalitet.

Regionen har som følge af de opstillede krav skabt ubegrundede hindringer for de økonomiske aktører og reelt favoriseret ét bestemt produkt. Udbuddet har dermed været skræddersyet med henblik på anskaffelsen af Palo Alto produkter.

Favoriseringen af Palo Alto-produkter er ikke objektivt begrundet, ligesom indkøbets størrelse (52.000 Endpoints (PC-klient) og 60.000 cloudbrugere til 90 firewall-licenser) er uproportionalt.

Det påhviler regionen at dokumentere, at opgavebeskrivelsen og behovsopgørelsen er sagligt begrundet. Denne bevisbyrde har regionen ikke løftet. De fremlagte rapporter mv. omfatter så vidt det ses ingen anbefalinger svarende til kravene fastsat i kravspecifikationen.

Der er ikke fremlagt dokumentation for, at regionen faktisk har truffet en strategisk beslutning om at anskaffe licenser på baggrund af saglige it-sikkerhedsmæssige hensyn, der kan forklare fastsættelsen af de omstridte krav.

ISO27001, Anneks A, kontrol A.12.4.1, som regionen henviser til, vedrører hændelseslogning generelt, men savner derudover sammenhæng til den indkøbte vare. CIS Controls v8, der er "et rammeværktøj med sikkerhedstiltag", indeholder en lang række forskellige anbefalinger til mulige sikkerhedstiltag, hvoraf et af dem, som fremhævet af regionen, angår indsamling af logs, mens et andet angår en anbefaling om at have anti-malware-beskyttelse på sin e-mailserver, herunder f.eks. bilagsscanning og/eller sandboxing. Det bestrides ikke, at det er hensigtsmæssigt at anvende hændelseslogning eller sandboxing generelt. Der fremgår imidlertid ikke nogen anbefalinger om, at firewallens indsamlede logs skal kunne hentes og anvendes af endpoint-beskyttelses-softwaren på den beskrevne måde i K12, eller at sandboxing skal kunne anvendes på den beskrevne måde i K18 og K19. Angivelserne fra virksomheden SentinelOne har alene præg af reklamemateriale for SentinelOnes produkter og kan derfor heller ikke tillægges nogen betydning.

Regionens manglende saglige behov for kun at ville købe produkter fra Palo Alto understreges endvidere af, at Trend Micro på nuværende tidspunkt er leverandør af endpoint-, og cloudbeskyttelsessoftware til regionen, hvorfor behovet for integration til Palo Alto-produkter ikke tidligere har været vigtigt for regionen. Dette understreger, at der i det tidligere påklagede udbud om endpoints og i det nu påklagede udbud angående endpoint-, cloudbeskyttelses- og SOAR-software er tale om, at regionen har truffet et teknologivalg baseret på Palo Alto-produkter og har skræddersyet sine anskaffelser herefter.

Kravene K12, K18 og K19 går væsentligt længere end nødvendigt med henblik på at opnå det ønskede sikkerhedsniveau. Kravene kan således formuleres leverandørneutralt og åbne for et bredere leverandørfelt og samtidig tilgodese det erklærede sikkerhedsniveau.

Både firewall- og sandkasse-løsninger er produkter, som findes i mange andre versioner på markedet, der kan opfylde regionens behov for IT-sikkerhed. Udbudsmaterialet indeholder dermed krav, som ikke står i et rimeligt forhold til det konkrete indkøb, og som går videre end, hvad der er nødvendigt for at imødekomme regionens konkrete saglige behov for endpoint-beskyttelsessoftware.

Til regionens anbringender om, at regionen af sikkerhedsmæssige, organisatoriske, tekniske og økonomiske grunde ønsker at bevare eksisterende 90 firewall-licenser og sandkasse-løsning, og at det vil være uhensigtsmæssigt at skulle udskifte regionens firewalls, bemærker Trend Micro, at virksomheden på nuværende tidspunkt er leverandør af den endpoint-beskyttelsessoftware, som nærværende udbud er til erstatning for, og at de opstillede krav effektivt vil betyde, at der skal ske en langt større udskiftning af software.

Henset til regionens erklærede mål om at forbedre sin it-sikkerhed kan det undre, at regionen vælger at forlange kompatibilitet med Palo Alto med det resultat, at Palo Alto-produkter vil blive tilbudt, når Palo Alto ifølge den uafhængige it-konsulentvirksomhed Gartner end ikke er blandt de 19 førende leverandører på markedet, jf. "Magic Quadrant for Endpoint Protection Platforms".

Region Hovedstaden har gjort gældende, at en ordregivende myndighed som altovervejende hovedregel er berettiget til at fastsætte de tekniske specifikationer, som den finder nødvendige og passende, og som er forbundet med kontraktens genstand, jf. udbudslovens § 40, stk. 4, § 42 og § 2. Det følger endvidere af lovbemærkningerne til udbudslovens § 40, stk. 4, at ordregiveren kan fastsætte de tekniske specifikationer, således at det alene er visse økonomiske aktører, der har adgang til udbuddet, når der er saglige grunde til at stille kravene. Herudover følger det af fast klagenævnspraksis, at ordregivere har et bredt skøn ved opgørelsen af deres indkøbsbehov og ved fastlæggelse af kravene til, hvordan disse behov skal opfyldes.

De fastsatte krav i opgavebeskrivelsen, herunder K12, K18 og K19, er sagligt begrundede og dermed i overensstemmelse med udbudslovens § 40, stk. 4, samt de grundlæggende principper om ligebehandling og proportionalitet i udbudslovens § 2. Det er sagligt og proportionalt, at Region Hovedstaden af

sikkerhedsmæssige, organisatoriske, tekniske og økonomiske grunde har ønsket at bevare sin eksisterende it-infrastruktur, herunder eksisterende firewalls og sandkasseløsning i videst muligt omfang.

Det vil indebære en betydelig meromkostning for Region Hovedstaden at udskifte alle sine firewalls, ligesom der også ville være en vis teknisk og organisatorisk, herunder driftsmæssig, risiko forbundet med omstillingen. Den tekniske risiko består bl.a. i, hvorledes en udskiftning vil passe ind i regionens arkitektur og opsætning, hvor opsætning af firewalls er en ret kompleks opgave.

En udskiftning vil – ud over omkostningerne til anskaffelsen – bl.a. afstedkomme et behov for opdatering af firewall-regler, politikker og vejledninger, hvilket vil være ressourcekrævende og udgøre en meromkostning. Herudover er det generelt anerkendt, at it-projekter er forbundet med risici, herunder forretningsmæssige, tekniske og økonomiske risici. Såfremt regionen i forbindelse med anskaffelsen af endpoint-software også skulle udskifte sine firewalls, ville det således afstedkomme yderligere risici og et forøget ressourceforbrug.

Region Hovedstadens eksisterende infrastruktur kan bidrage til realiseringen af regionens ønske om øget sikkerhed. Allerede og alene af denne grund er krav K12, K18 og K19 saglige og proportionale. Det er sagligt og proportionalt at stille krav om, at endpoint-softwaren kan udnytte de i krav K12 omhandlede logdata samt integrere mv. med sandkasseløsningen på den i K18 og K19 beskrevne måde, da dette er en effektiv måde at øge sikkerheden på. Kravet om at udnytte logdata understøttes bl.a. af ISO 27001, Anneks A "Referencekontrolmål og kontroller", kontrol A.12.4.1 vedrørende hændelseslogning, der foreskriver, at hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser skal udføres, opbevares og gennemgås regelmæssigt. Formålet med kontrol A.12.4.1 er generelt at registrere hændelser og tilvejebringe bevis i relation til potentielle og realiserede sikkerhedshændelser. Det følger også af analysen af regionens informationssikkerhed, CIS Control 08 "Audit Log Management", at det anbefales at indsamle detaljerede logs i tråd med det, der er fastsat i K12. Derudover er de fastsatte krav i K18 og K19 i tråd med CIS Control 09 "Email and Web Browser Protections", safeguard 9.6. Kravene om at gøre brug af regionens sandkasseløsning (sandboxing), jf. K18 og K19, understøttes endvidere af Center for Cybersikkerheds undersøgelsesrapport, "Anatomien af

målrettede ransomware-angreb". Kravene K12, K18 og K19 er fastlagt i tråd med substansen og teknikkerne i de anførte sikkerhedsforanstaltninger, som Digitaliseringsstyrelsen og Center for Cybersikkerhed har henvist til. Både CIS Controls og MITRE ATT&CK er udbredte og anerkendte ramme-værk, der bl.a. benyttes i vejledningsarbejdet af toneangivende danske myndigheder, hvilket yderligere understøtter, at der er tale om sagligt begrundede og proportionale krav.

Det er ikke korrekt, som anført af Trend Micro, at der ikke er truffet en strategisk beslutning om at anskaffe licenser. Beslutningen er truffet i forbindelse med udarbejdelsen og offentliggørelsen af udbudsmaterialet. Beslutningen er bl.a. baseret på analysen af regionens informationssikkerhed og Danske Regioners fælles målsætning, der begge er udtryk for analytiske og strategiske produkter, der skal understøtte en forbedring af sikkerheden i regionens organisation.

Atea A/S bød ind med endpoint-, cloudbeskyttelses- og SOAR-software fra producenten Microsoft og angav i den forbindelse, at "Atea og Microsoft imødekommer de stillede krav". Det fremgår af løsningsbeskrivelsen, at den tilbudte platform kan "integreres med 3. part, som f.eks. firewalls eller sagsbehandlingssystemer", ligesom der i løsningsbeskrivelsen udtrykkeligt henvises til integration relateret til Palo Alto. Atea A/S tilbød således "andet kendt endpoint- og cloudbeskyttelsessoftware". Det forhold, at Trend Micro ikke kan opfylde et konkret krav, eller at kravet alene kan opfyldes af en enkelt eller to leverandører eller producenter på markedet, indebærer ikke, at kravet er fastsat i strid med udbudslovens § 40, stk. 4, § 42 og § 2. Trend Micros påstand synes således primært at være baseret på, at Trend Micro selv ikke var i stand til at afgive tilbud. Et sagligt begrundet krav skal således ikke udgå, blot fordi kun én eller nogle få leverandører eller producenter vil kunne opfylde det. Efter udbudslovens § 40, stk. 4, og forarbejderne hertil er det tilladt at fastsætte saglige krav, herunder tekniske specifikationer, selvom det betyder, at alene visse økonomiske aktører afgiver tilbud. Ligebehandlingsprincippet stiller dermed ikke krav om, at ethvert vilkår i udbudsmaterialet skal være konkurrenceneutralt for alle aktører på markedet, og en ordregiver har således ikke pligt til at sænke sine krav til en ydelse som følge af, at kun én eller nogle få leverandører vil kunne levere det ønskede, hvis kravene i øvrigt er saglige.

Det er helt sædvanligt, at en organisation arbejder kontinuerligt med, hvordan analyser og strategier mest hensigtsmæssigt udmøntes, herunder hvordan udbud og kontrakter mest hensigtsmæssigt kan understøtte analyser og strategier. Det følger heraf, at den konkrete udmøntning af en analyse eller en strategi kan udvikle sig og variere over tid, fra projekt til projekt eller udbud til udbud. Det har i den forbindelse været afgørende, at den efterspurgte standardsoftware integreres med og udnytter regionens eksisterende it-infrastruktur i form af den eksisterende firewall og eksisterende sandkasseløsning.

Region Hovedstaden modtog mere end et tilbud, og der var således konkurrence om kontrakten. Atea A/S og Conscia Danmark A/S tilbød standardsoftware fra to forskellige producenter. Det er et udbredt fænomen på markedet for standardsoftware, at konkurrencen finder sted imellem forhandlere af software, der til tider tilbyder samme softwareprodukter. Dette er en konsekvens af udbredelsen af proprietær software på markedet og ikke udtryk for usaglige krav stillet af regionen. Det er normalt, at kunden ønsker, at allerede anskaffede produkter skal kunne sameksistere med henblik på at fastholde eller øge et allerede etableret sikkerhedsniveau. Et generelt krav om udskiftning af eksisterende it-infrastruktur ved køb af ny software er ikke rimeligt at pålægge ordregivende myndigheder. Det forhold, at der kun modtages få eller et enkelt tilbud under et udbud, er ikke nødvendigvis udtryk for, at der ikke har været tilstrækkelig konkurrence.

Vedrørende antallet af licenser har ordregivere et bredt skøn ved opgørelsen af deres indkøbsbehov og ved fastlæggelse af kravene til, hvordan disse behov skal opfyldes. Trend Micro synes at problematisere anskaffelsen af endpoint-licenser sammenholdt med regionens 90 firewall-licenser. Antallet af firewalls hænger bl.a. sammen med antallet af fysiske lokationer, mens antallet af endpoint-licenser hænger sammen med de omfattede antal endpoints (servere). Antallet af endpoint-licenser er derfor ikke knyttet til antallet af firewall-licenser. Fastsættelsen af det kvantitative behov for endpoint-licenser skal ses i lyset af, at der er tale om en omfattende og kompleks it-infrastruktur samt en kritisk anskaffelse, hvorfor størrelsen af regionens behov er behæftet med en vis usikkerhed.

Dertil kommer, at regionen ikke er forpligtet til at tillægge skifteomkostninger betydning, jf. klagenævnets kendelse af 26. maj 2011, Covergens A/S mod Viborg Kommune, ligesom der ikke er nogen juridiske hindringer for at

undlade at inddrage omstillingsomkostninger (skifteomkostninger) i tilbudsevalueringen, jf. Konkurrence- og Forbrugerstyrelsens vejledning "Totalomkostninger" (november 2016).

Ad påstand 2

Trend Micro har gjort gældende, at betingelserne for at annullere Region Hovedstadens beslutning om at tildele kontrakten om levering af endpoint-, cloudbeskyttelse og SOAR direkte til Conscia Danmark A/S er opfyldte som følge af overtrædelsen af de udbudsretlige regler, jf. det anførte ad påstand 1.

Region Hovedstaden har gjort gældende, at da Trend Micro ikke skal have medhold i påstand 1, jf. det anførte ad påstand 1, skal Trend Micro heller ikke have medhold i annullationspåstanden.

Ad påstand 3

Trend Micro har gjort gældende, at betingelserne for, at kontrakten mellem Region Hovedstaden og Conscia Danmark A/S skal erklæres for uden virkning, er opfyldt.

Kontrakten med Conscia Danmark A/S skal erklæres for uden virkning i medfør af lov om Klagenævnet for Udbud § 17, stk. 1, nr. 4, da kontrakten er indgået i strid med udbudslovens afsnit II, er baseret på et dynamisk indkøbssystem og den anslåede kontraktværdi overstiger tærskelværdien fastsat i disse regler.

Der er endvidere ikke grundlag for, at undtagelsesreglerne i § 17, stk. 2, kan finde anvendelse, da betingelserne herfor ikke er opfyldte. Regionen har ikke iagttaget sin forpligtelse efter § 17, stk. 2, nr. 1, ved alene at have underrettet de to tilbudsgivere om tildelingsbeslutningen, idet Trend Micro ligeledes må anses som "berørt" i klagenævnslovens forstand. Denne klagesag er den tredje klagesag mellem parterne inden for det seneste år, der alle har vedrørt det samme emne. Der har i perioden været jævnlig kontakt mellem parterne om regionens løbende udbud, som Trend Micro mener er en usaglig begunstigelse af en enkelt leverandør. Derudover har Trend Micro fulgt regionens tidligere udbud.

På grund af de opstillede krav i udbudsmaterialet, som klagenævnet kan lægge til grund ikke kunne opfyldes af Trend Micro, tjente det ikke noget formål for Trend Micro at indlevere et tilbud, som med sikkerhed ville blive afvist som ukonditionsmæssigt.

Da Trend Micro løbende har problematiseret udformningen af regionens kravspecifikationer, må Trend Micro derfor betragtes som en berørt tilbudsgiver i det konkrete udbud. Det forhold, at Trend Micro af logiske årsager ikke afgav tilbud på det konkrete udbud, bør ikke være afgørende for regionens pligt til at underrette Trend Micro om tildelingen. Det vil desuden stride mod formålet med indførelsen af standstill-perioden og dermed den effektive virkning af udbudsreglerne, såfremt Trend Micro ikke i det konkrete udbud skulle have meddelelse om tildelingen. Selvom trend Micro ikke er leverandør på SKI 02.06, forhandles Trend Micros produkter på SKI 02.06 af leverandører, som Trend Micro er underleverandør for. Det er således underordnet, om Trend Micro er leverandør på det omhandlende dynamiske indkøbssystem.

Der er ikke grundlag for at opretholde kontrakten i sin helhed med henvisning til klagenævnslovens § 17, stk. 3. Regionen står ikke i en situation, hvor regionen – hvis klagenævnet tager Trend Micros påstand til følge – ikke kan opretholde en høj grad af IT-sikkerhed. Således kan regionen som alternativ til opretholdelsen af den indgåede kontrakt med Conscia Danmark A/S forlænge de allerede eksisterende aftaler, som endnu ikke er udløbet. Der er dermed ikke tale om, at regionens systemer vil være ubeskyttede mod russiske hackere eller andre med tilsvarende hensigter.

Der er derfor heller ikke grundlag for at tage regionens tertiære synspunkt til følge, da det – henset til den eksisterende IT-infrastruktur hos regionen – ikke er nødvendigt først at implementere nærværende kontrakt for derefter at udbyde den på ny uden de ulovlige krav.

Region Hovedstaden har gjort gældende, at regionen har afholdt en frivillig standstill-periode i overensstemmelse med lov om Klagenævnet for Udbud § 3, herunder overholdt kravene til begrundelse og underretning i lov om Klagenævnet for Udbud § 2 og udbudslovens § 171, og kontrakten er indgået i overensstemmelse med udbudsreglerne. Der er derfor ikke belæg for at erklære kontrakten for uden virkning, jf. lov om Klagenævnet for Udbud § 17, stk. 2.

Region Hovedstaden har iagttaget sin forpligtelse efter § 17, stk. 2, nr. 1, ved at have underrettet de to tilbudsgivere om tildelingsbeslutningen. Trend Micro er ikke leverandør på SKI 02.06. Trend Micro er ikke berørt af beslutningen, idet Trend Micro hverken er tilbudsgiver eller ansøger.

Region Hovedstaden har subsidiært gjort gældende, at den pågældende kontrakt må opretholdes af hensyn til almenhedens interesser, jf. lov om Klagenævnet for Udbud, § 17, stk. 3, og derfor ikke kan erklæres for "uden virkning". Kontrakten vedrører antivirus-licenser til regionens slutbruger-PC'er (PC-klient) og cloudbrugere. Hvis den licenserede antivirus-software skal afinstalleres, såfremt kontrakten erklæres for uden virkning, vil slutbruger-PC'er (PC-klient) og cloudbrugere være sårbare med potentielt vidtrækkende konsekvenser for almenheden. Det følger af praksis fra klagenævnet, at en kontrakt nødvendigvis må opretholdes af hensyn til almenhedens interesser, jf. § 17, stk. 3, når f.eks. hensyn til at undgå konsekvenser for patienters sundhed taler herfor. I relation til det anskaffede antivirus-software er der tale om helt essentiel beskyttelse af regionens slutbruger-PC'er (PC-klient) og cloudbrugere samt kritiske it-systemer bl.a. på sundhedsområdet.

Opfyldelse af den udbudte kontrakt vedrørende levering af licenser til endpoint-, cloudbeskyttelse og SOAR samt tilknyttede ydelser er vigtig for regionen, idet de omhandlede slutbruger-PC'er (PC-klient) og cloudbrugere konkret bevæger sig i kritiske it-systemer, som understøtter hovedstadsområdets sundhedssektor, hvor det er essentielt, at slutbruger-PC'er (PC-klient) og cloudbrugere er beskyttede mod tab og læk af data, og at it-systemerne bevarer en stabil drift og dermed er tilgængelige.

Derudover er der bl.a. i lyset af konflikten mellem Rusland og Ukraine et øget behov for cybersikkerhed, herunder beskyttelse mod virusangreb, ransomware-, malware-, og spyware-infektion og andre former for digitale angreb. Forsvarets Efterretningstjenestes Center for Cybersikkerhed vurderer således i deres seneste trusselsvurdering, at cybertruslen fra cyberspionage og cyberkriminalitet er "MEGET HØJ".

Uden antivirus-software vil regionens slutbruger-PC'er (PC-klient) og cloudbrugere være mere sårbare, hvilket øger sandsynligheden for, at regionens kritiske it-systemer lammes i tilfælde af virusangreb, ransomware-infektion, malware og/eller spyware-infektion.

Såfremt kontrakten af 14. december 2022 erklæres for "uden virkning", har Region Hovedstaden mere subsidiært gjort gældende, at denne sanktion først skal træde i kraft, når regionen har haft mulighed for at anskaffe og installere antivirus-licenser til at erstatte de anskaffede antivirus-licenser ved kontrakten af 14. december 2022.

Ad påstand 4

Trend Micro har gjort gældende, at der er grundlag for at pålægge Region Hovedstaden en alternativ økonomisk sanktion, jf. klagenævnslovens § 19, stk. 2, nr. 6, såfremt klagenævnet ikke erklærer de indgåede kontrakter for uden virkning, jf. lovens § 17, eller kun erklærer kontrakterne for uden virkning for fremtiden, jf. § 18.

Såfremt kontrakten alene erklæres for delvis uden virkning, bør den del af kontrakten, der opretholdes, være så kortvarig som muligt inden for den gældende kontraktperiode. Hertil bør der idømmes en økonomisk sanktion for den del af kontrakten, der er blevet opretholdt. Dette gælder også, hvis kontrakten opretholdes efter lovens § 17, stk. 3.

Region Hovedstaden har gjort gældende, at anvendelse af lov om Klagenævnet for Udbud § 18, stk. 2, og §§ 19 eller 20 forudsætter, at kontrakten kan erklæres for uden virkning i henhold til lov om Klagenævnet for Udbud § 17, stk. 1, hvilket ikke er tilfældet. Der er derfor ikke belæg for at pålægge regionen en alternativ sanktion.

Klagenævnet udtaler

Ad påstand 1

Det følger af udbudslovens § 40, stk. 1 og 4, at de tekniske specifikationer, der er anført i udbudsmaterialet, skal give økonomiske aktører lige adgang til udbuddet og ikke må bevirke, at der skabes ubegrundede hindringer for, at et udbud åbnes for konkurrence.

Af forarbejderne til udbudslovens § 40, stk. 1, jf. lovforslag nr. 19 af 7. oktober 2015, fremgår bl.a.:

> ”Ordregiveren skal være særlig opmærksom på proportionalitetsprincippet i forbindelse med udarbejdelsen af de tekniske specifikationer, idet ordregiveren i henhold til proportionalitetsprincippet alene kan fastsætte krav, der er proportionale med kontraktens værdi og mål. Som følge heraf kan der alene fastsættes krav, der er nødvendige og passende for gennemførelsen af de tilsigtede formål.”

Endvidere fremgår det af forarbejderne til udbudslovens § 40, stk. 4, jf. lovforslag nr. 19 af 7. oktober 2015, bl.a.:

> ”I henhold til bestemmelsen i stk. 4 skal de tekniske specifikationer give økonomiske aktører lige adgang til udbuddet, og må ikke bevirke, at der skabes ubegrundede hindringer for, at et udbud åbnes for konkurrence.
>
> Bestemmelsen medfører, at ordregiveren ved udarbejdelse af de tekniske specifikationer, skal sikre en lige adgang til udbudsproceduren for de økonomiske aktører. Bestemmelsen er et udtryk for ligebehandlingsprincippet i § 2, hvorefter ensartede forhold ikke må behandles forskelligt, og at forskellige forhold ikke må behandles ensartet, medmindre en sådan forskellig behandling er objektivt begrundet og proportionalt. Som følge heraf kan ordregiveren fastsætte de tekniske specifikationer, således det alene er visse økonomiske aktører, der har adgang til udbuddet, hvis disse krav er saglige. Ensartede økonomiske aktører skal dog have en lige adgang til udbudsproceduren.
>
> Endvidere må ordregiveren ikke i de tekniske specifikationer skabe ubegrundede hindringer for konkurrencen eller på andre måder kunstigt indsnævre konkurrencen.
>
> Som følge heraf vil det alene være muligt for ordregiveren at fastsætte krav til tekniske specifikationer, som har en konkurrencebegrænsende virkning, hvis ordregiveren kan anføre saglige grunde til at stille kravene.”

Region Hovedstaden har i de tekniske specifikationer stillet krav om, at tilbudt endpoint-beskyttelsessoftware skal 1) kunne hente og anvende firewallgenererede logdata fra Region Hovedstadens Palo Alto firewalls (Krav 12), 2) integrere til og benytte Region Hovedstadens Palo Alto sandkasseløsning (Krav 18) og 3) sende alle ukendte “Portable executable files” på endpoints til Region Hovedstadens Palo Alto sandkasseløsning (Krav 19).

Der er således i de tekniske specifikationer stillet krav om, at det indkøbte software skal være kompatibelt med regionens eksisterende firewalls og sandkasseløsning. De stillede krav medfører en indsnævring i konkurrencen,

derved at kravene udelukker en række softwareprodukter, herunder endpoint-beskyttelsessoftwaren fra Trend Micro.

Region Hovedstaden har som begrundelse for at fastsætte de tekniske specifikationer anført, at regionen med kravene i K12, K18 og K19 har til hensigt at bevare og udnytte den eksisterende infrastruktur, herunder firewalls og sandkasseløsning, for derved bl.a. at bidrage til øget it-sikkerhed. Regionen har endvidere anført, at såfremt regionen i forbindelse med anskaffelsen af endpoint-software skulle udskifte sine firewalls, ville det afstedkomme yderligere risici og et forøget ressourceforbrug.

Efter fast klagenævnspraksis er det ordregivers valg, hvordan kontraktgenstanden skal defineres. En ordregiver fastsætter således inden for de rammer, der følger af udbudsreglerne, bl.a. hvorledes de udbudte ydelser skal beskrives, og hvilke krav der skal stilles til ydelserne. Ordregiveren kan i den forbindelse, jf. forarbejderne til udbudslovens § 40, stk. 4, fastsætte de tekniske specifikationer, således at det alene er visse økonomiske aktører, der har adgang til udbuddet, hvis disse krav er saglige. Endvidere må ordregiveren ikke i de tekniske specifikationer skabe ubegrundede hindringer for konkurrencen eller på andre måder kunstigt indsnævre konkurrencen.

Det ligger fast, at det er ordregiveren, som skal bevise, at de stillede krav er sagligt begrundede og proportionale i forhold til kontraktens værdi og mål.

Jakob O. Ebbensgaard udtaler herefter:

Jeg finder, at det var sagligt begrundet, at Region Hovedstaden ved anskaffelse af endpoint-beskyttelsessoftware tog hensyn til ønsket om at bevare og udnytte den eksisterende infrastruktur, herunder firewalls og sandkasseløsning, for derved at bidrage til øget it-sikkerhed og minimere risici, og jeg finder, at kravene i K12, K18 og K19 ikke går væsentligt længere end nødvendigt med henblik på at opnå det ønskede sikkerhedsniveau.

Kravene i K12, K18 og K19 er derfor i overensstemmelse med udbudslovens § 2, og det er min vurdering, at de fastsatte krav er sagligt begrundede og proportionale.

Jeg stemmer derfor for ikke at tage påstanden til følge.

Maria Haugaard udtaler:

I henhold til forarbejderne til udbudslovens § 40 skal ordregiver som følge af proportionalitetsprincippet sikre, at de stillede krav er nødvendige og passende.

Uanset at regionen har et bredt skøn ved tilrettelæggelsen af udbud, ved opgørelsen af sit indkøbsbehov og ved fastlæggelse af kravene til, hvordan regionens behov opfyldes, finder jeg desuagtet, at regionen ikke i tilstrækkelig grad har redegjort for, hvorfor de stillede krav er nødvendige og saglige.

Regionen henviser til, at den eksisterende it-infrastruktur skal bevares af "sikkerhedsmæssige, organisatoriske, tekniske og økonomiske grunde", ligesom regionen skriver, at den "eksisterende infrastruktur kan bidrage til realiseringen af regionens ønske om øget sikkerhed. Allerede og alene af denne grund er krav K12, K18 og K19 saglige og proportionale."

Øget sikkerhed er et væsentlig hensyn, men jeg finder, at regionen ikke ved disse generelle vendinger har redegjort for, hvorfor kravene er sagligt begrundede og proportionale, og hvorfor der alene ved denne kravfastsættelse kan sikres den ønskede sikkerhed. Når der stilles krav om snitflader til eksisterende firewalls og sandkasseløsninger, bør det vurderes, om disse krav er proportionale med det, som skal købes. I den forbindelse ses på, at der erhverves software-beskyttelse af 52.000 endpoints og 60.000 cloudbrugere, som alle kræver snitflader til de to beskrevne Palo Alto-produkter.

Det er oplyst, at der i dette udbud er to tilbudsgivere, som har tilbudt software fra to forskellige producenter. Det er dog ikke afklaret, om der ud fra den måde, hvorpå kravene er formuleret, reelt kun kan leveres produkter fra én producent. Dette skærper kravene til regionens bevisbyrde, og regionen bør derfor kunne redegøre for, at de stillede krav var proportionale, nødvendige og sagligt begrundede. At der er indkommet to tilbud er i sig selv ikke ensbetydende med, at kravene til fastsættelse af tekniske specifikationer i udbudslovens § 40 er opfyldt. Det må være ordregiver, som fastsætter de tekniske specifikationer, som bærer bevisbyrden for, at de stillede krav er sagligt begrundede og proportionale.

Jeg finder på den baggrund, og som sagen er oplyst for klagenævnet, at regionen ikke har løftet sin bevisbyrde.

Jeg stemmer derfor for at tage påstanden til følge.

Da formandens stemme er udslagsgivende ved stemmelighed, tager klagenævnet ikke påstanden til følge.

Ad påstand 2, 3 og 4

Efter det, der er anført ad påstand 1, er der ikke grundlag for at tage påstandene til følge.

Herefter bestemmes:

Klagen tages ikke til følge.

Filial af Trend Micro Emea Limited skal i sagsomkostninger til Region Hovedstaden betale 40.000 kr., der betales inden 14 dage efter modtagelsen af denne kendelse.

Klagegebyret tilbagebetales ikke.

Jakob O. Ebbensgaard

Genpartens rigtighed bekræftes.

Katrine K. Gade
Overassistent