Region Hovedstaden

Center for It, Medico og Telefoni

POLITIKERSPØRGSMÅL

Journal-nr.: 18038947

Dato: 21. august 2018

Spørgsmål nr.: 125-18
Dato: 10. august 2018
Stillet af: Niels Høiby og Jakob Rosenberg
Besvarelse udsendt den: 21. august 2018

Spørgsmål:
Vi vil gerne gentage vores politikerspørgsmål fra april vedrørende en godkendt revisionserklæring om it sikkerheden hos Sundhedsplatformens leverandør Epic, se nedenfor, som iflg svaret skulle være leveret 18. maj 2018:

Er revisionserklæringen modtaget fra Epic og hvornår? Hvis den er modtaget vil vi gerne have aktindsigt og derfor modtage den til gennemlæsning.

Svar:
Administrationen henviser til den aktuelle orientering, der blev udsendt den 17. august 2018 til regionsrådet samt til "Notat til RR vedr. fortrolighed i forbindelse med Epics revisionserklæring", som blev sendt til regionsrådet den 21. august 2018.

Det kan oplyses, at regionsrådets medlemmer har kunnet se revisionserklæringen i Sekretariatet den 21. august 2018 mellem kl. 15-17 umiddelbart op til regionsrådsmødet.

Det kan oplyses, at revisionserklæringen ikke er udsendt til regionsrådets medlemmer, idet administrationen har vurderet, at regionsrådsmedlemmerne hver især bør kunne forholde sig til, om de selv ønsker at være i besiddelse af den fortrolige revisionserklæring. Medlemmerne kan dog anmode om sagsindsigt i erklæringen efter kommunestyrelseslovens § 9, herunder om at få revisionserklæringen tilsendt. Dette har indtil videre to medlemmer gjort.

Der arbejdes pt. på at udarbejde et ledelsesresume af revisionserklæringen. Denne version vil være åben og vil derfor være tilgængelig i forbindelse med aktindsigtsanmodninger mv. Så snart ledelsesresumeet er færdigt og godkendt vil det blive udsendt til regionsrådet.

Region Hovedstaden

Center for It, Medico og Telefoni

ORIENTERING

Journal-nr.: 18038246

Til: Regionsrådet

Dato: 17. august 2018

Godkendt revisionserklæring fra Epic om informationssikkerhed

Epic er forpligtet til én gang årligt at levere en revisionserklæring om deres efterlevelse af informationssikkerhed. Erklæringen skal ifølge kontrakten være baseret på en række standardundersøgelser, der forholder sig til Epics generelle datasikkerhed, når Epic tilgår Region Hovedstadens data. Revisionserklæringen skulle være leveret den 22. juni 2017.

Revisionserklæringen har pga. forsinkelsen tidligere været omtalt i pressen, og i svar på politikerspørgsmål. Administrationen har derudover i henholdsvis maj og juni 2018 modtaget en række anmodninger om aktindsigt i Epics revisionserklæring. Af hensyn til Region Hovedstadens fortrolighedsforpligtelse over for Epic, samt Offentlighedsloven § 30, stk. 2, kan selve revisionserklæringen dog ikke udleveres i sin helhed. Revisionserklæringen er pt. igen omtalt i nogle medier.

Administrationen modtog den 23. maj 2018 Epics revisionserklæring om informationssikkerhed, som er udarbejdet af et eksternt revisionsfirma (PwC US) og dækker perioden den 28. april 2016 til den 31. december 2017.

Administrationen har i fællesskab med Region Hovedstadens eget revisionsfirma (BDO) gennemgået revisionsrapporten, hvortil administrationen havde en række opklarende spørgsmål af mere formel karakter. Epic har i løbet af sommeren 2018 fremsendt dokumentation på de områder i revisionsrapporten, som administrationen har haft spørgsmål til.

Administrationen har nu modtaget disse opfølgende svar, og kan endeligt konkludere, at der er leveret en revisionserklæring fra ekstern revisor (PwC US), der belyser de målepunkter, som er aftalt.

Revisionserklæringen blev godkendt af administrationen den 16. august 2018.

Region Hovedstaden

Center for It, Medico og Telefoni

NOTAT

Journal-nr.: 18038246

Til: Regionsrådet

Dato: 21. august 2018

Fortrolighed i forbindelse med Epics revisionserklæring

Regionsrådet har udbedt sig en uddybende forklaring omkring fortrolighedsforholdene vedrørende Epics revisionserklæring, hvilket hermed følger.

Efter lov om offentlighed i forvaltningen § 30, nr. 2, omfatter retten til aktindsigt ikke oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig økonomisk betydning for den person eller virksomhed, oplysningerne angår, at anmodningen ikke imødekommes.

Det er administrationens klare opfattelse, at Epics revisionserklæring er omfattet af de typer oplysninger, der nævnes i bestemmelsen.

Af lovbemærkningerne fremgår, at der for sådanne oplysninger gælder en klar formodning for, at udlevering af oplysningerne vil indebære en nærliggende risiko for, at virksomheden eller den person, oplysningerne angår, vil lide skade af betydning, men at der dog bør indhentes en udtalelse fra den, oplysningerne angår, for at få belyst risikoen for, at en udlevering af oplysninger om forretningsforhold m.v. vil medføre den nævnte risiko for økonomisk skade.

Ved anmodning om aktindsigt i oplysninger af den nævnte karakter, indhenter administrationen derfor en udtalelse fra den pågældende virksomhed. Region Hovedstaden foretog i overensstemmelse hermed en høring af Epic, da regionen i sommeren 2018 modtog en række aktindsigtsanmodninger i revisionserklæringen af 23. maj 2018.

På baggrund af høringen bad Epic om at undtage alle dele af revisionsrapporten bortset fra følgebrevet. Epic bad om at få oplysninger undtaget af følgende årsager:

- Rapporten indeholder beskrivelser af Epics tekniske og organisatoriske sikkerhedsforanstaltninger. En offentliggørelse af disse vil forøge risikoen for sikkerhedsbrud markant, idet indsigt i indretningen af sådanne foranstaltninger, vil kunne have afgørende betydning for en ondsindet persons evne til at "bryde ind" i Sundhedsplatformen eller i Epics lignende løsninger. Ethvert sikkerhedsbrud må forventes at medføre betydelig økonomisk skade for Epic

og potentielt dennes kunder. Økonomisk skade vil eksempelvis kunne bestå af Epics og dennes kunders interne ressourcer, der er nødvendige for at håndtere sikkerhedsbruddet samt erstatningskrav fra Epics kunder og borgere (datasubjekter).

- En offentliggørelse af rapporten vil kunne give Epics konkurrenter et værdifuldt indblik i Epics metoder og fremgangsmåder i forhold til indretning af tekniske og organisatoriske sikkerhedsforanstaltninger, der er nødvendige for leverandører på markedet hvor Epic opererer. Epics konkurrenter vil ved rapportens fulde offentliggørelse eksempelvis opnå en konkurrencefordel i forhold til løsning af egne udfordringer vedrørende indretning af påkrævede tekniske og organisatoriske sikkerhedsforanstaltninger. Endvidere vil Epics konkurrenter opnå en konkurrencefordel, når de gives muligheden for at kunne kopiere Epics fremgangsmåde til at dokumentere deres sikkerhed. Som anført i pkt. 3 nedenfor vil enhver konkurrencefordel medføre en nærliggende risiko for betydelig økonomisk skade.
- Markedet for software-løsninger til sundhedssektoren, hvori Epic opererer, er et marked præget af hård konkurrence. Store og strategisk vigtige ordrer tildeles oftest ved udbud, hvor marginaler kan være afgørende for udfaldet. Konkurrencefordele for Epics konkurrenter vil derfor potentielt kunne være afgørende for, hvorvidt Epic vinder et givent udbud. I tilfælde hvor Epic ikke vinder, vil Epic for det første gå glip af den fremtidige profit, der var forbundet med den givne ordre, og for det andet vil Epic have båret omkostninger til afgivelse af tilbud forgæves.

På baggrund af Epics udtalelse er det administrationens vurdering, at der ifølge offentlighedslovens §30, nr. 2 er hjemmel til at undtage revisionserklæringen i sin helhed (når bortses fra overskrift og datering), og at hensynet til at Epic ikke påføres økonomisk skade, herunder i konkurrencemæssig henseende, er til hinder for, at der kan gives meroffentlighed i revisionserklæringen efter offentlighedslovens § 14. Det er samtidig administrationens vurdering, at de pågældende hensyn medfører, at oplysningerne er omfattet af tavshedspligt, jf. forvaltningslovens § 27, stk. 1, nr. 2.

Det bemærkes endvidere, at en offentliggørelse ville udgøre et brud på den i kontrakten med Epic aftalte tavshedspligt, som potentielt ville kunne føre til, at Epic kunne rejse sag mod Region Hovedstaden med påstand om en større erstatningsforpligtelse.

Administrationen skal derfor indskærpe, at revisionserklæringen er et fortroligt dokument og ikke må videreformidles. Dette med undtagelse af følgebrevet til revisionserklæringen, hvor alle oplysninger må offentliggøres, dog med undtagelse af Stirling Martins signatur.

Revisionserklæringen er ikke udsendt til regionsrådets medlemmer, idet administrationen har vurderet, at regionsrådsmedlemmerne hver især bør kunne forholde sig til, om de selv ønsker at være i besiddelse af den fortrolige revisionserklæring. Medlemmerne

kan dog anmode om sagsindsigt i erklæringen efter kommunestyrelseslovens § 9, herunder om at få revisionserklæringen tilsendt. Dette har indtil videre to medlemmer gjort.

Der arbejdes pt. på at udarbejde et ledelsesresume af revisionserklæringen.
Denne version vil være åben og vil derfor være tilgængelig i forbindelse med aktindsigtsanmodninger mv. Så snart ledelsesresumeet er færdigt og godkendt vil det blive udsendt til regionsrådet.