

Sundheds- og Ældreministeriet
Holbergsgade 6
1057 København K



Dato 14-08-2020

Sagsbehandler Birgitte Aaberg

birgitte.aaberg@stab.rm.dk

Tel. Sagsnr. 1-51-70-1-20

Side 1

Udtalelse fra regionsrådet i forbindelse med ministerredegørelse

Sundheds- og Ældreministeren har bedt om regionsrådets udtalelse til Statsrevisorernes beretning nr. 15/2019 om outsourcete persondata, jf. mailbrev af 19. maj 2020.

Regionsrådet har noteret sig beretningens indhold og særligt de kritikpunkter, som er aktuelle ift. Region Midtjylland. Regionsrådet har noteret sig, at Statsrevisorernes kritik i forhold til Region Midtjylland falder i følgende tre hovedgrupper: *risikovurdering af databehandlere, databehandleraftaler og tilsyn med databehandlere.*

Regionsrådet vil nedenfor forholde sig til kritikken i forhold til disse hovedgrupper, herunder hvilke overvejelser og tiltag kritikken har givet anledning.

Vedrørende risikovurdering af databehandlere

Regionsrådet har noteret sig den kritik Statsrevisorerne har udtalt i forhold til manglende risikovurdering af regionens databehandlere.

Region Midtjylland har i mange år arbejdet med en central risikovurdering i henhold til den internationale informationssikkerhedsstandard ISO27001 ift. regionens forretningskritiske it-systemer. Region Midtjylland har siden 25. maj 2018 arbejdet med konsekvensanalyser for de registrerede (DPIA).

Herudover har Region Midtjylland i forbindelse med udarbejdelse af databehandleraftalerne foretaget såvel en juridisk som it-sikkerhedsmæssig vurdering af de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger.

Databehandleraftalens vilkår er en udmøntning af denne vurdering.

Region Midtjylland har i sit høringssvar til Rigsrevisionen gjort opmærksom på, at Region Midtjylland ikke er enig i Rigsrevisionens vurdering af kravet om risikovurdering før 25. maj 2018.

Desuagtet tager Region Midtjylland Statsrevisorernes kritik til efterretning, herunder at Statsrevisorerne ikke har fundet, at Region Midtjylland på tilstrækkelig vis har kunnet dokumentere risikovurderingen.

I regi af Region Midtjyllands Handleplan for Informationssikkerhed er der under initiativet "Informationssikkerhed fra start" nedsat en arbejdsgruppe med henblik på at sikre, at der i forbindelse med behandling af personoplysninger foretages en vurdering af de risici behandlingen af personoplysninger medfører, og at denne risikovurdering dokumenteres.

Samtidig har Region Midtjylland via af Tværregional Styregruppe for Informationssikkerhed (TSI) sammen med de øvrige regioner nedsat en arbejdsgruppe, der skal undersøge, om det vil være muligt for regionerne at udvikle og anvende et fælles værktøj til risikovurdering af databehandlere.

Allerede nu har regionen tilpasset sin skabelon til databehandlerinstruks, så det mere tydeligt kan dokumenteres, at der er foretaget en konkret vurdering af databehandlerens tekniske og organisatoriske sikkerhedsforanstaltning i forbindelse med databehandleraftalen.

Vedrørende databehandleraftaler

Regionsrådet tager Statsrevisorernes kritik i forhold til manglende databehandleraftaler alvorligt.

Region Midtjylland arbejder kontinuerligt med at indgå de nødvendige databehandleraftaler i relation til it-systemer, forskningsprojekter mv.

Region Midtjylland bemærker, at Region Midtjylland adskiller sig fra de øvrige undersøgte myndigheder i forhold til antallet af databehandleraftaler, myndigheder skal have. Dette skyldes dels regionens komplekse systemlandskab, og dels omfanget af databehandlinger, som finder sted i regionen, herunder i forbindelse med patientbehandling, forskning og administrativ sagsbehandling. Hertil kommer, at regionen har oplevet særlige udfordringer med at indgå databehandleraftaler i forhold til legacy systemer (f.eks. ældre it-systemer og udstyr, som ikke overholder tidssvarende standarder for sikkerhed), hvor der kan være tale om systemer, der understøtter livsvigtig patientbehandling og hvor der kun er enkelte eller ganske få udbydere. Disse udfordringer er nationalt kendt, og adresseres i Strategi for cyber- og informationssikkerhed i sundhedssektoren 2019-2022.

Region Midtjylland har siden iværksættelse af Rigsrevisionens undersøgelse arbejdet med at indgå databehandleraftaler på systemer omfattet af undersøgelsen, og regionen er snart i mål.

Region Midtjylland har samtidig iværksat et arbejde med en digitaliseret proces for databehandleraftaleindgåelse, hvorved vi håber at kunne minimere sagsbehandlingstiden på databehandleraftaler og derved håndtere en større volumen af databehandleraftaler på kortere tid.

Vedrørende tilsyn med databehandlere

Region Midtjylland tager Statsrevisorernes kritik til efterretning.

Regionens Informationssikkerhedsudvalg har i april 2019 godkendt en tilsynsstrategi for netop databehandlere (Model for passende kontrolforanstaltninger af databehandlere).

Denne tilsynsstrategi har betydet, at regionen er blevet mere opmærksom på, at der allerede i forbindelse med indkøb/udbud stilles krav om levering af en revisionserklæring med henblik på iagttagelse af regionens tilsynsforpligtelse overfor leverandøren som databehandler.

Tilsynsstrategien er udmøntet i en ny intern proces i Region Midtjylland, som sikrer en mere formaliseret tilgang og dokumentation af kontrol og opfølgning med regionens databehandlere.

På grundlag af Rigsrevisionens undersøgelse har Region Midtjylland iværksat tilsyn med databehandlerne på de systemer, som var i scope for rigsrevisionens undersøgelse.

Herudover har Region Midtjylland vedtaget en tilsynsplan for regionens databehandlere for 2020, hvor der i 2., 3. og 4. kvartal gennemføres tilsyn og opfølgning med databehandlere på regionens kritiske systemer samt yderligere et antal databehandlere årligt ud fra en risikobaseret tilgang.

Samtidig har regionerne via af Tværregional Styregruppe for Informationssikkerhed (TSI) aftalt et samarbejde omkring tilsyn med de databehandlere, som alle eller flere regioner anvender. Ligesom der er nedsat en tværregional arbejdsgruppe med henblik på at klarlægge, hvordan regionerne sikrer et tilfredsstillende tilsyn med hinanden som databehandlere, samt sikre at der stilles de rette krav i fælles tværregionale udbud.

Venlig hilsen



Anders Kühnau
Regionsrådsformand