SUNDHEDS-
OG ÆLDREMINISTERIET

Holbergsgade 6
DK-1057 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Sundheds- og ældreministeren

Statsrevisorerne Sekretariatet
Prins Jørgens Gård 2, Folketinget, Christiansborg
ministersvar@ft.dk
1240 København K
DK, Danmark

Dato: 22-09-2020
Enhed: PEM
Sagsbeh.: DEPPHM
Sagsnr.: 1904657
Dok. nr.: 1379188

Sundheds- og ældreministerens redegørelse til Statsrevisorerne vedr. Rigsrevisionens beretning nr. 15/2019 om outsourcede persondata

Statsrevisorerne har den 15. maj 2020 fremsendt beretning nr. 15/2019 om outsourcede persondata.

Denne redegørelse vedrører beretningens undersøgelse og konklusioner om 10 udvalgte, outsourcede it-systemer, der indeholder følsomme eller fortrolige personoplysninger fra henholdsvis Sundhedsdatastyrelsen, Styrelsen for Patientsikkerhed, Sundhedsstyrelsen, Statens Serum Institut og Lægemiddelsstyrelsen.

Til brug for denne redegørelse er der indhentet udtalelse fra regionsrådet i Region Midtjylland, jf. § 18, stk. 3 i lov om revisionen af statens regnskaber m.v. Udtalelsen er vedlagt som bilag.

Indledningsvist vil jeg gerne kvittere for, at beretningen sætter fokus på en væsentlig databeskyttelsesretlig dagsorden. Den øgede digitalisering inden for sundhedsvæsenet stiller store krav til it-sikkerheden og til beskyttelsen af de personoplysninger, der indgår i de digitale løsninger. Samtidig medfører den øgede digitalisering, at der i stadig stigende grad anvendes eksterne it-leverandører og underleverandører. Derfor skal vi stille store krav til en god og solid leverandørstyring i sundhedsvæsenet.

Jeg har noteret mig, at Rigsrevisionens undersøgelse og Statsrevisorernes kritik falder i følgende tre kategorier: Udarbejdelse af risikovurderinger, indgåelse af databehandleraftaler og tilsyn med databehandlere.

Ad. Risikovurderinger:
Det fremgår af beretningens figur 4 på s. 16, at Sundheds- og Ældreministeriet har foretaget risikovurderinger for fem af de ti it-systemer, der indgår i beretningsundersøgelsen. Heraf er risikovurderingen for to af de fem it-systemer udarbejdet efter der er indgået en databehandleraftale.

Jeg finder det naturligvis ikke tilfredsstillende, at der ikke rettidigt er udarbejdet risikovurderinger for mere end halvdelen af de it-systemer, der indgår i beretningsundersøgelsen.

Ad. Databehandleraftaler:
Af beretningens figur 5, på side 19 fremgår det, at Sundheds- og Ældreministeriet har haft en rettidig indgået databehandleraftale med 7 af 10 databehandlere.

Det er naturligvis ikke tilfredsstillende og derfor finder jeg det positivt, at sundhedsdatastyrelsen har oplyst, at der arbejdes på indgåelse af en databehandleraftale for National Service Platform, hvori der vil være et selvstændigt afsnit om behandlingen af personoplysninger i forbindelse med Organdonorregisteret. Databehandleraftalen for de to systemer forventes at blive underskrevet i september 2020

Ad. Tilsyn:
Det fremgår af beretningens figur 6 på s. 24, at Sundheds- og Ældreministeriet ikke har haft en plan for gennemførelsen af tilsyn med databehandlere for syv ud af de ti udvalgte it-systemer.

Af beretningens figur 7, på s. 25, fremgår det endvidere, at der er ført tilsyn med tre af fem it-systemer, der har en databehandleraftale som er mere end et år gammel.

Jeg finder det utilfredsstillende, at der ikke findes en tilsynsplan for alle ministeriets databehandlere samt, at der kun er udført tilsyn med tre ud af fem it-systemer, hvor databehandleraftalen har haft en varighed på mere end et år.

Nyt koncept for leverandørstyring i Sundheds- og Ældreministeriets koncern
For at sikre en bedre leverandørstyring, arbejdes der internt i Sundheds- og Ældreministeriet på udformningen af et koncept for leverandørstyring, der tilgodeser alle faser heraf - lige fra risikovurdering over kontraktindgåelse til tilsyn med leverandørerne.

Formålet med konceptet er at systematisere arbejdet med leverandørstyringen, så der fremover sker en rettidig udarbejdelse af risikovurderinger og indgåelse af databehandleraftaler samt at fastsættelsen af foranstaltninger i databehandleraftalen sker på baggrund af risikovurderingen.

Det kommende leverandørstyringskoncept hjælper ligeledes den dataansvarlige styrelse til at forholde sig til tilsynsforpligtelsen. Formålet hermed er at sikre, at der allerede i forbindelse med kontraktindgåelsesfasen bliver taget stilling til hvilken type tilsyn der skal udføres, og hvordan.

Konceptet vil ligeledes understøtte den dataansvarlige styrelses arbejde med at beskrive alle leverandørens forpligtelser i forhold til evt. underdatabehandlere.

Rigsrevisionens undersøgelse om outsourcede persondata har desuden afstedkommet, at der i departementets årlige tilsyn med informationssikkerheden hos ministeriets styrelser, sættes fokus på leverandørstyring, og i særdeleshed på områderne; risikovurderinger, databehandleraftaler samt tilsyn og opfølgning.

Jeg finder det positivt, at der med et initiativ som et samlet leverandørstyringskoncept, sættes fokus på alle faser af leverandørstyringen i Sundheds- og Ældreministeriets koncern. Jeg forventer, at konceptet kan afstedkomme en systematisk og stringent tilgang til arbejdet med risikovurderinger, databehandleraftaler og tilsyn med leverandører i Sundheds- og Ældreministeriets koncern.

Region Midtjyllands bemærkninger:

Statsrevisorerne bemærker, at Region Midtjylland har haft en kritisabel styring af eksterne databehandlere. Det fremgår endvidere af beretningens boks 1 på s. 17, at Region Midtjylland anvender en privat databehandler til at sende elektroniske breve, og at regionen ikke havde udarbejdet en risikovurdering forinden systemet blev outsourcet.

Jeg finder det naturligvis utilfredsstillende at Region Midtjylland ikke har en bedre styring af deres eksterne databehandlere.

Region Midtjylland har oplyst, at der er nedsat en arbejdsgruppe, der har til formål at sikre, at der udarbejdes en risikovurdering, når det er aktuelt, samt at dette dokumenteres.

Regionen Midtjylland har desuden oplyst, at regionens databehandleraftaleskabelon er tilpasset således, at det mere tydeligt kan dokumenteres, at der er foretaget en konkret vurdering af databehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger.

Region Midtjylland har endvidere oplyst, at regionen siden Rigsrevisionens undersøgelse, har arbejdet med at indgå databehandleraftaler for de it-systemer, var omfattet af beretningsundersøgelsen, og hvor der ikke var indgået databehandleraftaler.

I forhold til kritikken for manglende tilsyn med databehandlere har regionen oplyst, at regionen i forbindelse med indkøb og udbud er blevet mere opmærksom på at stille krav om levering af revisionserklæring, så regionens tilsynsforpligtelse iagttages.

Regionen har vedtaget en tilsynsplan for 2020 for regionens kritiske systemer, samt iværksat tilsyn med databehandlerne på de systemer, som var omfattet af Rigsrevisionens undersøgelse.

Jeg finder det positivt, at Region Midtjylland giver udtryk for, at regionen allerede har igangsat et arbejde med at forbedre leverandørstyringen og f.eks. allerede har igangsat arbejdet med at indgå de manglende databehandleraftaler og har opdateret deres interne skabelon for indgåelse af databehandleraftaler samt har udarbejdet en tilsynsplan og har igangsat en række tilsyn.

Kopi af denne redegørelse er sendt til Rigsrevisionen på rr@rigsrevisionen.dk.

Med venlig hilsen

Magnus Heunicke