FOLKETINGET
RIGSREVISIONEN

August 2024

Rigsrevisionens notat om
beretning om

outsourcede persondata

Opfølgning i sagen om outsourcede persondata (beretning nr. 15/2019)

27. juni 2024

RN 306/24

I. Baggrund og konklusion

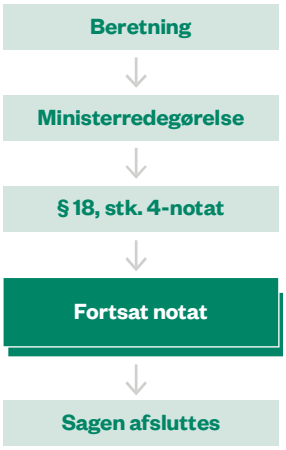
1. Rigsrevisionen følger i dette notat op på sagen om outsourcede persondata, som blev indledt med en beretning i 2020. Opfølgningen sker med henblik på at vurdere, om ministeriernes initiativer adresserer den kritik, der fremgår af Statsrevisorernes bemærkninger og Rigsrevisionens beretning. Vi har tidligere behandlet sagen i notater til Statsrevisorerne af 4. november 2020 og 20. maj 2022.

2. Beretningen handlede om 17 ministeriers og Region Midtjyllands indsats for at sikre, at borgeres følsomme og fortrolige persondata behandles sikkert, når myndighederne outsourcer opbevaringen af data til en ekstern databehandler. Vi undersøgte, om myndighederne havde udarbejdet risikovurderinger, indgået databehandleraftaler og ført tilsyn med deres databehandlere. Vi undersøgte desuden, om Justitsministeriet, herunder Datatilsynet, og Finansministeriet havde understøttet de øvrige myndigheders styring af databehandlere ved at udgive relevante vejledninger. Endelig undersøgte vi, om Datatilsynet havde ført et risikobaseret tilsyn.

3. Da Statsrevisorerne behandlede beretningen, fandt de det meget alvorligt, at myndighedernes styring ikke havde sikret, at outsourcede følsomme og fortrolige persondata opbevares sikkert hos eksterne databehandlere. Statsrevisorerne påtalte i den forbindelse, at myndighederne ikke havde overholdt reglerne om databeskyttelse. Der gælder bl.a. krav om at udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn med databehandlerne. Kravene har været gældende siden 2000. Statsrevisorerne bemærkede, at særligt Udlændinge- og Integrationsministeriet og Region Midtjylland havde haft en kritisabel styring af databehandlere. Finansministeriet havde haft den bedste styring.

Det fremgik også af beretningen, at Datatilsynet ikke havde ført et risikobaseret tilsyn.

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

Databehandler
En databehandler er den juridiske eller fysiske person, private virksomhed, offentlige myndighed mv., som behandler personoplysninger på vegne af den dataansvarlige. Databehandleren har adgang til at behandle data, men bestemmer hverken formål med behandlingen, eller hvordan behandlingen sker. Databehandleren handler kun på baggrund af instruks fra den dataansvarlige.

Konklusion

Alle de myndigheder, der indgik i undersøgelsen, har nu udarbejdet risikovurderinger i forbindelse med, at de har outsourcet opbevaringen af følsomme eller fortrolige persondata.

Skatteministeriet og Region Midtjylland, der ikke havde udarbejdet risikovurderinger for alle undersøgte it-systemer ved den seneste opfølgning, har nu også foretaget de relevante risikovurderinger. Rigsrevisionen finder dette tilfredsstillende.

Rigsrevisionen finder det ligeledes tilfredsstillende, at Datatilsynet har arbejdet med at udvikle tilsynets risikobaserede tilgang. Datatilsynet har arbejdet på 8 initiativer fra strategien 2020-2023, som skulle styrke en risikobaseret tilgang. Datatilsynet fortsætter med at styrke indsatsen i 2024-2026 bl.a. ved at videreføre indsatsen på flere initiativer fra tilsynsstrategien fra 2020-2023. Rigsrevisionen vurderer, at Datatilsynet har arbejdet med og er godt på vej mod et risikobaseret tilsyn.

Rigsrevisionen vurderer på den baggrund, at sagen kan afsluttes.

II. Status på sagen

4. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkter:

Et opfølgningspunkt afsluttes, når Statsrevisorerne på baggrund af indstilling fra Rigsrevisionen vurderer, at myndighedernes initiativer er tilfredsstillende.

Opfølgningspunkt	Status
1. Myndighedernes indsats med at udarbejde risikovurderinger, når de outsourcer opbevaringen af følsomme eller fortrolige persondata.	Afsluttet for 3 ud af de 18 myndigheder i forbindelse med notat til Statsrevisorerne af 4. november 2020. Afsluttet for yderligere 13 myndigheder i forbindelse med notat til Statsrevisorerne af 20. maj 2022. I dette notat følges der op på de resterende 2 myndigheder (Skatteministeriet og Region Midtjylland). Punktet afsluttes for de sidste 2 myndigheder.
2. Myndighedernes indsats med at indgå databehandleraftaler med deres databehandlere, som opbevarer følsomme eller fortrolige persondata.	Afsluttet for 14 ud af de 18 myndigheder i forbindelse med notat til Statsrevisorerne af 4. november 2020. Afsluttet for de resterende 4 myndigheder i forbindelse med notat til Statsrevisorerne af 20. maj 2022.
3. Myndighedernes indsats med at udføre tilsyn med deres databehandlere, som opbevarer følsomme eller fortrolige persondata.	Afsluttet for 7 ud af de 18 myndigheder i forbindelse med notat til Statsrevisorerne af 4. november 2020. Afsluttet for de resterende 11 myndigheder i forbindelse med notat til Statsrevisorerne af 20. maj 2022.
4. Justitsministeriets, herunder Datatilsynet, og Finansministeriets indsats med at understøtte de øvrige myndigheders styring af databehandlere.	Afsluttet i forbindelse med notat til Statsrevisorerne af 4. november 2020.
5. Datatilsynets arbejde med at indføre et risikobaseret tilsyn, herunder Datatilsynets implementering af de 8 indsatser i Datatilsynets nuværende strategi.	Behandles og afsluttes i dette notat.

III. Skatteministeriets, Region Midtjyllands og Datatilsynets initiativer

5. Vi gennemgår i det følgende Skatteministeriets, Region Midtjyllands og Datatilsynets initiativer i forhold til de udestående opfølgningspunkter.

6. Opfølgningen er baseret på dokumentgennemgang, redegørelser og dialog med de reviderede.

Myndighedernes udarbejdelse af risikovurderinger

7. Statsrevisorerne hæftede sig ved, at myndighederne for 58 % af de it-systemer, der indgik i undersøgelsen, ikke havde udarbejdet en risikovurdering, inden de havde indgået en databehandleraftale. Myndighederne havde således ikke grundlag for at fastsætte passende sikkerhedsforanstaltninger eller planlægge deres tilsyn.

Det fremgik af beretningen, at 17 ud af de 18 undersøgte myndigheder – med Kulturministeriet som eneste undtagelse – manglede at udarbejde risikovurderinger for ét eller flere systemer.

Vores opfølgning i maj 2022 viste, at Region Midtjylland og Skatteministeriet fortsat ikke havde udarbejdet risikovurderinger for henholdsvis 5 og 3 af de undersøgte it-systemer.

Vores opfølgning nu viser, at såvel Skatteministeriet som Region Midtjylland har gennemført risikovurderinger for de it-systemer, der ikke var risikovurderet ved den seneste opfølgning, og som fortsat er i drift. Dermed har alle myndigheder, der indgik i undersøgelsen, udarbejdet risikovurderinger.

Datatilsynets tilsyn

8. Statsrevisorerne hæftede sig ved, at Datatilsynet ikke havde ført et risikobaseret tilsyn og ikke havde opdateret sin strategi, siden GDPR trådte i kraft i maj 2018. Datatilsynet havde heller ikke gennemført de tilsyn hos offentlige myndigheder og private virksomheder, som var planlagt. Det har medført en lav risiko for at blive opdaget i overtrædelser af databeskyttelsesreglerne.

Det fremgik af beretningen, at den manglende dokumentation for risikobaseret planlægning af tilsynet betød, at det var usikkert, om Datatilsynet havde anvendt de tilgængelige resurser til at føre tilsyn, der hvor risikoen var størst.

9. Vi konstaterede ved opfølgningen i maj 2022, at Datatilsynet havde udarbejdet en strategi for at gennemføre en data- og risikobaseret kontrolindsats, og at Datatilsynet havde iværksat alle de 8 initiativer i strategien, som Datatilsynet havde planlagt. Ét initiativ var afsluttet, 3 var delvist gennemført, og 4 initiativer var igangsat, men der var endnu ikke konkrete fremskridt eller en opdateret tidsplan. De 8 initiativer var:

1. Evaluering af datakvaliteten og registrering af metadata.
2. Systematiseret indsamling af data.
3. Forsøg med nyt tilsynskoncept.
4. Adgang til eksterne datakilder.
5. Klare kriterier for udvælgelse af kontrolområder.
6. Flere databaserede beslutninger.
7. Dokumenterede processer, beslutninger og resultater.
8. Forsøg med effektmåling.

10. Vores opfølgning viser, at Datatilsynet har arbejdet på alle de 8 initiativer fra strategien 2020-2023. Bl.a. har Datatilsynet på forsøgsbasis tilrettelagt kontrolaktiviteter på baggrund af data om risiko. Datatilsynet vil dog fortsætte med at forbedre den risikobaserede tilgang og viderefører nogle initiativer i tilsynsstrategien for 2024-2026. I den ny strategi indgår bl.a. et fortsat arbejde med at forbedre egne data og anvendelsen af eksterne data, videreudvikling af en model til effektiv og risikobaseret udvælgelse af kontrolområder og videreudvikling af metoder til at vurdere effekten af kontrolaktiviteter.

11. Hele sagen kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

Birgitte Hansen