



**FOLKETINGET
RIGSREVISIONEN**

November 2020

**Rigsrevisionens notat om
beretning om**

**outsourcete
persondata**

Vedrører:**Statsrevisorernes beretning nr. 15/2019 om outsourcete persondata**

4. november 2020

RN 310/20

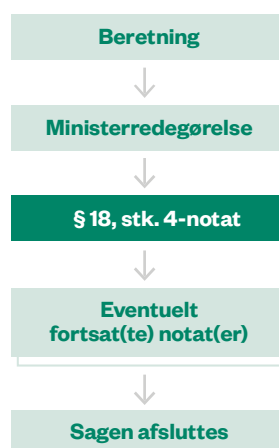
Ministeren for fødevarer, fiskeri og ligestilling og ministeren for nordisk samarbejdes redegørelse af 24. august 2020
Udlændinge- og integrationsministerens redegørelse af 2. september 2020
Statsministerens redegørelse af 3. september
Forsvarsministerens redegørelse af 8. september 2020
Miljøministerens redegørelse af 14. september 2020
Social- og indenrigsministerens redegørelse af 15. september 2020
Erhvervsministerens redegørelse af 17. september 2020
Kirkeministerens redegørelse af 17. september 2020
Klima-, energi- og forsyningsministerens redegørelse af 19. september 2020
Finansministerens redegørelse af 21. september 2020
Justitsministerens redegørelse af 21. september 2020
Skatteministerens redegørelse af 21. september 2020
Uddannelses- og forskningsministerens redegørelse af 21. september 2020
Sundheds- og ældreministerens redegørelse af 22. september 2020
Transportministerens og boligministerens redegørelse af 22. september 2020
Beskæftigelsesministerens redegørelse af 24. september 2020
Børne- og undervisningsministerens redegørelse af 27. september 2020
Kulturministerens redegørelse af 5. oktober 2020

1. Rigsrevisionen vurderer i dette notat de initiativer, som ministrene vil iværksætte som følge af Statsrevisorernes bemærkninger og beretningens konklusioner.

**Konklusion**

Flere ministre oplyser, at de finder det positivt, at Rigsrevisionen har sat fokus på et vigtigt område, og at beretningen har givet anledning til en række konkrete initiativer og handleplaner i deres arbejde med at forbedre beskyttelsen af følsomme og fortrolige personoplysninger. Størstedelen af myndighederne oplyser, at de med udgangspunkt i beretningen har iværksat initiativer, der skal sikre en hensigtsmæssig styring af deres databehandlere, med fokus på udarbejdelse af risikovurderinger, indgåelse af databehandleraftaler samt udførelse af og opfølgning på tilsyn.

Sagsforløb for en større undersøgelse



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

Myndighederne

”Myndighederne” er i denne undersøgelse de 17 ministerier, som indgår i undersøgelsen, og Region Midtjylland.

Rigsrevisionen finder Børne- og Undervisningsministeriets og Statsministeriets initiativerne i forhold til styring af databehandlere tilfredsstillende og vurderer, at denne del af sagen for de 2 myndigheder kan afsluttes.

Justitsministeren og finansministeren oplyser, at de er enige i, at det ville have været hensigtsmæssigt, hvis alle 20 vejledninger om databeskyttelse var udkommet, inden GDPR blev gældende den 25. maj 2018. Samtidig oplyser justitsministeren, at bekendtgørelsen og vejledningen om lokationskravet (tidligere krigsreglen) nu er offentliggjort. Rigsrevisionen finder dette tilfredsstillende og vurderer, at denne del af sagen kan afsluttes.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Beskæftigelsesministeriets, Erhvervsministeriets, Finansministeriets, Forsvarsministeriets, Justitsministeriets, Kirkeministeriets, Klima-, Energi- og Forsyningsministeriets, Miljø- og Fødevarerministeriets, Region Midtjyllands, Skatteministeriets, Social- og Indenrigsministeriets, Sundheds- og Ældreministeriets, Transport- og Boligministeriets og Uddannelses- og Forskningsministeriets indsats med at udarbejde risikovurderinger
- Erhvervsministeriets, Justitsministeriets, Region Midtjyllands og Sundheds- og Ældreministeriets indsats med at indgå databehandleraftaler
- Beskæftigelsesministeriets, Finansministeriets, Forsvarsministeriets, Justitsministeriets, Klima-, Energi- og Forsyningsministeriets, Kulturministeriets, Region Midtjyllands, Sundheds- og Ældreministeriets, Transport- og Boligministeriets, Uddannelses- og Forskningsministeriets og Udlændinge- og Integrationsministeriets indsats med at udføre tilsyn
- Datatilsynets arbejde med at indføre et risikobaseret tilsyn.

I. Baggrund

2. Rigsrevisionen afgav i maj 2020 en beretning om outsourcete persondata. Beretningen handlede om 17 ministeriers og Region Midtjyllands indsats for at sikre, at borgernes 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, og om Datatilsynet havde ført et risikobaseret tilsyn.

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

Statsrevisorerne fandt det utilfredsstillende, at Justitsministeriet, herunder Datatilsynet, og Finansministeriet ikke i tilstrækkelig grad havde understøttet de øvrige myndigheders styring af databehandlere.

Undersøgelsen viste, at myndighederne først havde udgivet 8 ud af 20 relevante vejledninger, efter at GDPR var blevet gældende den 25. maj 2018. Justitsministeriet havde ved beretningens offentliggørelse endnu ikke udgivet hverken bekendtgørelse eller vejledning om lokationskravet (tidligere krigsreglen), som bestemmer, hvilke it-systemer der af hensyn til statens sikkerhed ikke må opbevares uden for Danmark.

Det fremgik også af beretningen, at Datatilsynet ikke havde ført et risikobaseret tilsyn. Det var derfor usikkert, om Datatilsynet havde anvendt sine tilgængelige resurser til at føre tilsyn, hvor risikoen er størst.

4. Hele sagen og dens dokumenter kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

II. Gennemgang af myndighedernes redegørelser

Myndighedernes udarbejdelse af risikovurderinger

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

Det fremgik af beretningen, at en række af myndighederne havde udarbejdet en række risikovurderinger efter indgåelse af databehandleraftaler, så der ved afslutningen på den undersøgte periode i september 2019 manglede risikovurderinger for 42 % af de 148 undersøgte systemer. 17 ud af 18 myndigheder i undersøgelsen – med Kulturministeriet som undtagelse – manglede at udarbejde risikovurderinger for ét eller flere systemer.

6. Statsministeren oplyser, at ministeriet har udarbejdet den risikovurdering, som ministeriet manglede i undersøgelsen. Børne- og undervisningsministeren og udlændinge- og integrationsministeren oplyser, at deres ministerier har gennemgået hele deres systemportefølje og udarbejdet de manglende risikovurderinger.

7. Beskæftigelsesministeren og justitsministeren oplyser, at deres ministerier er i gang med at udarbejde de manglende risikovurderinger for deres it-systemer i undersøgelsen, og erhvervsministeren oplyser, at ministeriet er i gang med at udarbejde de manglende risikovurderinger på tværs af ministeriets koncern.

Social-og indenrigsministeren oplyser, at ministeriet vil tage skridt til, at ministeriets it-ansvarlige kan sikre, at alle it-systemer med outsourcete persondata overholder databeskyttelsesreglerne. Klima-, energi- og forsyningsministeren oplyser, at ministeriet er i gang med at udarbejde nye retningslinjer for udarbejdelse af risikovurderinger. Finansministeren oplyser, at ministeriet har været opmærksom på at prioritere en målrettet GDPR-implementering, og at gennemsigtighed i behandling af persondata er vigtig i forhold til at skabe tryghed og tillid til de fællesoffentlige it-systemer og dermed sikre opbakning til den offentlige digitalisering.

Skatteministeren oplyser, at han har igangsat en screening af hele sin systemportefølje for at udarbejde de manglende risikovurderinger, som forventes afsluttet i 2021. Forsvarsministeren oplyser, at ministeriet siden undersøgelsen har gennemgået de berørte it-systemer og har nedbragt antallet af uregelmæssigheder.

Sundheds- og ældreministeren oplyser, at ministeriet arbejder på et samlet koncept for leverandørstyring, herunder risikovurdering, og transportministeren og boligministeren oplyser, at ministeriet arbejder på at sætte øget fokus på de registreredes rettigheder.

Rigsrevisionen konstaterer, at Kirkeministeriet, Miljø- og Fødevarerministeriet, Region Midtjylland og Uddannelses- og Forskningsministeriet har igangsat initiativer, der skal sikre et forbedret arbejde med at udarbejde risikovurderinger fremover. Rigsrevisionen konstaterer dog også, at disse myndigheder ikke beskriver konkrete tiltag, og at tiltagene ikke er afsluttede.

8. Rigsrevisionen finder Statsministeriets, Børne- og Undervisningsministeriets og Udlændinge- og Integrationsministeriets initiativer tilfredsstillende og vurderer, at sagen kan afsluttes for de 3 myndigheder.

9. Rigsrevisionen vil fortsat følge denne del af sagen for de resterende 14 myndigheder, der endnu ikke har afsluttet arbejdet.

10. Rigsrevisionen kan i øvrigt konstatere, at beretningen har givet anledning til en række øvrige initiativer til at imødegå Rigsrevisionens kritikpunkter i beretningen, hvad angår risikovurderinger. Tabel 1 viser myndighedernes initiativer og tiltag.

Tabel 1**Myndighedernes initiativer og tiltag til bedre arbejde med risikovurderinger**

Initiativer	Myndigheder (igangsatte initiativer)	Myndigheder (afsluttede initiativer)
Nyt risikovurderingskoncept	Sundheds- og Ældreministeriet Uddannelses- og Forskningsministeriet	Børne- og Undervisningsministeriet Erhvervsministeriet
Indskærpet retningslinjer for risikovurderinger/leverandørforhold	Justitsministeriet Klima-, Energi- og Forsyningsministeriet Kirkeministeriet Transport- og Boligministeriet	
Indskærpet fokus på de registreredes rettigheder	Beskæftigelsesministeriet Uddannelses- og Forskningsministeriet	
Nye organisatoriske tiltag (nye afdelinger eller arbejdsgrupper)		Forsvarsministeriet Region Midtjylland

Det fremgår af tabel 1, at flere myndigheder har oplyst, at der er iværksat en række øvrige initiativer, som skal styrke deres arbejde med at udarbejde risikovurdering fremover. Fx har Børne- og Undervisningsministeriet og Erhvervsministeriet indført nye risikovurderingskoncepter, og Forsvarsministeriet og Region Midtjylland har oprettet nye afdelinger eller nedsat arbejdsgrupper, der skal styrke arbejdet med at udarbejde risikovurderinger.

Myndighedernes indgåelse af databehandleraftaler

11. Statsrevisorerne hæftede sig ved, at myndighederne ikke havde indgået en databehandleraftale for 14 % af it-systemerne, selv om de havde outsourcet opbevaringen af følsomme eller fortrolige persondata.

Det fremgik af beretningen, at flere af myndighederne indgik nye databehandleraftaler undervejs i undersøgelsen, så der kun manglede databehandleraftaler for 9 % af it-systemerne ved undersøgelsesperiodens afslutning i september 2019. 5 ud af 18 myndigheder manglede at indgå én eller flere databehandleraftaler for deres systemer ved undersøgelsens afslutning. Det drejede sig om Erhvervsministeriet, Justitsministeriet, Region Midtjylland, Sundheds- og Ældreministeriet og Udlændinge- og Integrationsministeriet.

12. Udlændinge- og integrationsministeren oplyser, at ministeriet har gennemgået hele sin systemportefølje og nu har indgået alle manglende databehandleraftaler.

13. Erhvervsministeren, justitsministeren og sundheds- og ældreministeren oplyser, at deres ministerier og Region Midtjylland arbejder på at indgå de resterende databehandleraftaler for de manglende systemer i undersøgelsen og samtidig arbejder på andre relevante initiativer.

14. Rigsrevisionen finder udlændige- og integrationsministerens initiativer tilfredsstillende og vurderer, at denne del af sagen kan afsluttes.

15. Rigsrevisionen vil forsat følge de 4 øvrige myndigheders arbejde med at få indgået databehandleraftaler på de systemer, der var en del af Rigsrevisionens undersøgelse.

16. Rigsrevisionen kan i øvrigt konstatere, at beretningen har givet anledning til en række øvrige initiativer til at imødegå Rigsrevisionens kritikpunkter i beretningen for så vidt angår databehandleraftaler. Tabel 2 viser myndighedernes initiativer og tiltag.

Tabel 2
Myndighederne initiativer og tiltag i arbejdet med databehandleraftaler

Initiativer	Myndigheder (igangsatte initiativer)	Myndigheder (afsluttede initiativer)
Indskærpet retningslinjer for databehandleraftaler eller leverandørforhold generelt	Beskæftigelsesministeriet Justitsministeriet Region Midtjylland Sundheds- og Ældreministeriet	Uddannelses- og Forskningsministeriet
Indgå manglende databehandleraftaler for relevante it-systemer på tværs af organisationen	Udlændinge- og Integrationsministeriet Kirkeministeriet	Børne- og Undervisningsministeriet
Nye organisatoriske tiltag (nye afdelinger eller arbejdsgrupper)		Forsvarsministeriet
Hensigtserklæring om at forbedre arbejdet med databehandleraftaler/leverandørstyring generelt (ikke konkrete tiltag)	Kulturministeriet Miljø- og Fødevarerministeriet Social- og Indenrigsministeriet	

Det fremgår af tabel 2, at flere myndigheder har oplyst, at de har taget en række øvrige initiativer. Fx har Uddannelses- og Forskningsministeriet udarbejdet nye retningslinjer for indgåelse af databehandleraftaler, og 4 øvrige myndigheder har igangsat sådan et arbejde.

Myndighedernes udførelse af tilsyn

17. Statsrevisorerne hæftede sig ved, at myndighederne ikke har ført tilsyn med databehandlerne for 23 % af systemerne og dermed ikke havde undersøgt, om databehandlerne overholder vilkårene i databehandleraftalen og databeskyttelsesreglerne.

Det fremgik af beretningen, at 11 ud af 18 myndigheder manglede at føre tilsyn med én eller flere af deres databehandlere, selv om databehandleraftalen var indgået mere end 1 år før undersøgelsestidspunktet. Der drejer sig om Beskæftigelsesministeriet, Finansministeriet, Forsvarsministeriet, Justitsministeriet, Klima-, Energi- og Forsyningsministeriet, Kulturministeriet, Region Midtjylland, Sundheds- og Ældreministeriet, Transport- og Boligministeriet, Uddannelses- og Forskningsministeriet og Udlændinge- og Integrationsministeriet.

18. Rigsrevisionen konstaterer, at ingen af de 11 myndigheder endnu har afsluttet tilsyn med alle de resterende databehandlere, der indgik i undersøgelsen.

19. Finansministeren oplyser, at ministeriet vil styrke tilsynsmodellen, og klima-, energi- og forsyningsministeren oplyser, at ministeriet nu udarbejder handleplaner for tilsyn med databehandlere og underdatabehandlere med udgangspunkt i de specifikke risikovurderinger. Forsvarsministeren og justitsministeren oplyser, at deres ministerier er ved at rette op på alle mangler i undersøgelsen. Transportministeren og boligministeren oplyser, at ministeriet har igangsat et arbejde, der skal sikre systematisk og dokumenteret tilsyn med databehandlere og underdatabehandlere.

Udlændinge- og integrationsministeren oplyser, at ministeriet har igangsat tilsyn i hele ministeriets koncern. Sundheds- og ældreministeren oplyser, at Region Midtjylland har igangsat tilsyn med de resterende databehandlere fra undersøgelsen, og at regionen samtidig har vedtaget en ny tilsynsstrategi og tilsynsplan for 2020. Beskæftigelsesministeren, sundheds- og ældreministeren og uddannelses- og forskningsministeren oplyser, at deres respektive ministerier har igangsat initiativer med at udarbejde nye tilsynskoncepter eller forbedre eksisterende koncepter.

Rigsrevisionen konstaterer, at Kulturministeriet ikke har iværksat konkrete initiativer til at føre tilsyn med sine databehandlere eller udvikle et tilsynskoncept, samtidig med at ministeriet ikke havde ført tilsyn for nogen af sine databehandlere i undersøgelsen.

20. Rigsrevisionen kan konstatere, at ingen af de 11 myndigheder har iværksat alle initiativer endnu eller afsluttet tilsynet med de resterende databehandlere, der indgik i undersøgelsen. Rigsrevisionen vil derfor fortsat følge de 11 myndigheder arbejde med at føre tilsyn med deres databehandlere.

21. Rigsrevisionen kan i øvrigt konstatere, at beretningen har givet anledning til en række øvrige initiativer til at sikre, at der bliver ført tilsyn med myndighedernes databehandlere, som opbevarer følsomme eller fortrolige personoplysninger. Tabel 3 viser myndighedernes initiativer og tiltag.

Tabel 3
Myndighederne initiativer og tiltag i arbejdet med at føre tilsyn

Initiativer	Myndigheder (igangsatte initiativer)	Myndigheder (afsluttede initiativer)
Nyt eller skærpet tilsynskoncept eller koncepter for leverandørstyring generelt	Beskæftigelsesministeriet Erhvervsministeriet Finansministeriet Justitsministeriet Klima-, Energi- og Forsyningsministeriet Sundheds- og Ældreministeriet Uddannelses- og Forskningsministeriet Justitsministeriet	Børne- og Undervisningsministeriet Region Midtjylland
Føre tilsyn med relevante systemer på tværs af organisationen	Skatteministeriet Udlændinge- og Integrationsministeriet	
Nye organisatoriske tiltag (nye afdelinger eller arbejdsgrupper)	Forsvarsministeriet Klima-, Energi- og Forsyningsministeriet	
Hensigtserklæring om at forbedre arbejdet med at føre tilsyn/leverandørstyring generelt (ikke konkrete tiltag)	Kulturministeriet Miljø- og Fødevarerministeriet Social- og Indenrigsministeriet Transport- og Boligministeriet	

Det fremgår af tabel 3, at en række myndigheder har iværksat eller afsluttet initiativer med at udarbejde nye tilsynskoncepter, koncepter for bedre leverandørstyring i koncernen generelt eller nye organisatoriske tiltag.

Justitsministeriets, herunder Datatilsynets, og Finansministeriets vejledningsindsats

22. Statsrevisorerne hæftede sig ved, at væsentlige vejledninger fra Justitsministeriet og Finansministeriet først udkom, efter at myndighederne skulle have implementeret GDPR. Statsrevisorerne bemærkede også, at Justitsministeriet ikke havde udgivet hverken en bekendtgørelse eller en vejledning om lokationskravet, som bestemmer, hvilke it-systemer der af hensyn til statens sikkerhed skal opbevares i Danmark.

Det fremgik af beretningen, at 8 ud af 20 relevante vejledninger om beskyttelse af personoplysninger først udkom, efter GDPR blev gældende den 25. maj 2018, herunder væsentlige vejledninger om udarbejdelse af risikovurderinger og brug af cloud-tjenester.

23. Finansministeren er enig i, at forsinkelsen af vejledningen om cloud-services har været u hensigtsmæssig, men at Digitaliseringsstyrelsen har lagt vægt på, at vejledningen skulle være retvisende på udgivelsestidspunktet og bl.a. afventede vejledningen om lokationskravet fra Justitsministeriet.

Justitsministeren oplyser, at ministeriet grundlæggende er enig i, at det ville have været hensigtsmæssigt, hvis alle vejledninger var udkommet, inden GDPR fik virkning, men bemærker, at myndighederne principielt ikke var forpligtede til at udgive vejledninger. Ministeren oplyser også, at Datatilsynet har erkendt, at der er et stort vejledningsbehov, og overvejer, hvordan Datatilsynet kan øge omfanget af vejledning og sikre, at vejledningerne bliver mere konkrete, uden at det går ud over tilsynets øvrige opgaver. Endelig oplyser ministeren, at bekendtgørelsen og vejledningen om lokationskravet udkom i juni 2020.

24. Rigsrevisionen finder det tilfredsstillende, at Justitsministeriet har udgivet en bekendtgørelse og vejledning om lokationskravet, og at Datatilsynet arbejder aktivt på at forbedre sin vejledningsindsats over for øvrige myndigheder fremover. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

Datatilsynets tilsyn

25. Statsrevisorerne hæftede sig ved, at Datatilsynet ikke havde ført et risikobaseret tilsyn og ikke havde opdateret sin strategi, siden GDPR blev gældende 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 risikobaserede planlægning af tilsyn betød, at det er usikkert, om Datatilsynet har anvendt de tilgængelige resurser til at føre tilsyn, der hvor risikoen er størst. Det fremgik også af beretningen, at Datatilsynet kun havde afsluttet 8 tilsyn med offentlige myndigheder fra 25. maj 2018 til og med udgangen af 2019. Hvis Datatilsynet havde afsluttet 80 % af sine planlagte tilsyn inden for 6 måneder, som er tilsynets målsætning, kunne Datatilsynet have afsluttet mindst 50 tilsyn i denne periode. Det betyder, at der er få afgørelser, som myndighederne kan benytte som fortolkningsbidrag til at opfylde GDPR.

26. Justitsministeren oplyser, at Datatilsynet har taget Rigsrevisionens bemærkninger til efterretning. Datatilsynet har også oplyst, at Datatilsynet på nuværende tidspunkt kun i beskedent omfang har adgang til data, der gør det muligt at karakterisere Datatilsynets tilsyn som databaseret, og at Datatilsynet ikke besidder medarbejderkompetencer til at kunne bearbejde data i større omfang. Datatilsynet har på den baggrund iværksat et arbejde, som samlet set skal understøtte, at tilsynet i højere grad føres "de rigtige steder", og at tilsynets aktiviteter har den størst mulige præventive effekt. Datatilsynet skal i den forbindelse bl.a. have øget adgang til relevante datakilder, højere datakvalitet og kvalificeret brug af data.

27. Rigsrevisionen finder det positivt, at Datatilsynet vil øge sin brug af relevante datakilder til at gøre sit tilsyn mere risikobaseret og dermed understøtte, at tilsynet udføres de steder, hvor risikoen er størst. Rigsrevisionen vil fortsat følge denne del af sagen.