FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

Maj 2020
– 15/2019

Rigsrevisionens beretning afgivet til Folketinget med Statsrevisorernes bemærkninger

Outsourcede persondata

15/2019

Beretning om

outsourcede persondata

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

København 2020

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:

Statsrevisorerne fremsender med deres bemærkning Rigsrevisionens beretning til Folketinget og vedkommende minister.

Alle ministre undtagen udenrigsministeren afgiver en redegørelse til beretningen.

Rigsrevisor afgiver et notat med bemærkninger til ministrenes redegørelser.

På baggrund af ministrenes redegørelser og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i november 2020.

Ministrenes redegørelser, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2019, som afgives i februar 2021.

Statsrevisorernes bemærkning tager udgangspunkt i denne karakterskala:

Karakterskala	
Positiv kritik	• finder det meget/særdeles positivt • finder det positivt • finder det tilfredsstillende/er tilfredse med
Kritik under middel	• finder det ikke helt tilfredsstillende
Middel kritik	• finder det utilfredsstillende/er utilfredse med • påpeger/understreger/henstiller/forventer • beklager/finder det bekymrende/foruroligende
Skarp kritik	• kritiserer/finder det kritisabelt/kritiserer skarpt/og indskærper • påtaler/påtaler skarpt
Skarpeste kritik	• påtaler skarpt og henleder særligt Folketingets opmærksomhed på

Henvendelse vedrørende denne publikation rettes til:
Statsrevisorerne
Folketinget
Christiansborg
1240 København K

Tlf.: 3337 5987
statsrevisorerne@ft.dk
www.ft.dk/statsrevisorerne

Yderligere eksemplarer kan købes ved henvendelse til:
Rosendahls Lager og Logistik
Vandtårnsvej 83A
2860 Søborg

Tlf.: 4322 7300
distribution@rosendahls.dk
www.rosendahls.dk

ISSN 2245-3008
ISBN trykt 978-87-7434-663-0
ISBN online 978-87-7434-664-7

Statsrevisorernes bemærkning

Beretning om outsourcede persondata

Danmark er et af de mest digitaliserede lande i verden. Digitaliseringen betyder, at de offentlige myndigheder indsamler og behandler mange oplysninger om borgerne. En stor del af oplysningerne er af følsom eller fortrolig karakter. Det kan derfor have store negative konsekvenser for såvel den enkelte borger som for den offentlige forvaltning, hvis oplysningerne ender i de forkerte hænder eller går tabt.

Danmark er blandt de lande i EU, som outsourcer den største andel af statslige it-systemer. Outsourcing betyder, at en opgave, fx drift, vedligeholdelse og udvikling af it-tjenester, overlades til en ekstern leverandør, fx en privat virksomhed eller en anden offentlig myndighed. Outsourcing muliggør på den ene side billigere drift og bedre udnyttelse af ekspertise, men ændrer samtidig styringsopgaven fra at være operationel til at være en kontraktbaseret styring af relationen til de eksterne databehandlere. I denne undersøgelse har Rigsrevisionen gennemgået 148 it-systemer, hvor opbevaringen af persondata er outsourcet af myndigheder på alle ministerområder, undtagen Udenrigsministeriet, og af Region Midtjylland.

Statsrevisorerne påtaler og finder det meget alvorligt, at myndighedernes styring ikke har sikret, at outsourcede følsomme og fortrolige persondata opbevares sikkert hos de eksterne databehandlere. Statsrevisorerne påtaler i den forbindelse, at myndighederne ikke har overholdt reglerne om databeskyttelse, herunder krav om at udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn med databehandlerne, som har været gældende siden 2000.

Statsrevisorerne bemærker, at særligt Udlændinge- og Integrationsministeriet og Region Midtjylland har haft en kritisabel styring af eksterne databehandlere, mens Finansministeriet har haft den bedste styring af databehandlere.

Statsrevisorerne

15. maj 2020

Henrik Thorup*
Klaus Frandsen
Villum Christensen
Frank Aaen
Britt Bager
Flemming Møller Mortensen

* Statsrevisor Henrik Thorup har ikke deltaget ved behandlingen af denne sag på grund af inhabilitet.

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

Statsrevisorerne har hæftet sig ved disse resultater fra undersøgelsen:

- Myndighederne har ikke udarbejdet en risikovurdering, inden de har indgået en databehandleraftale, for 58 % af de it-systemer, der indgår i undersøgelsen. Myndighederne har således ikke haft grundlag for at fastsætte passende sikkerhedsforanstaltninger eller planlægge deres tilsyn.
- Myndighederne har kun i 6 ud af 17 tilfælde, hvor de benytter globale cloud-udbydere til at opbevare persondata, udarbejdet en risikovurdering, og flere myndigheder har i øvrigt ikke haft fuld klarhed over indholdet af de standardvilkår, som de har accepteret.
- Myndighederne har ikke indgået en databehandleraftale for 14 % af it-systemerne, selv om de har outsourcet opbevaringen af følsomme eller fortrolige persondata.
- Myndighederne har ikke ført tilsyn med databehandlerne for 23 % af systemerne og har ikke undersøgt, om databehandlerne overholder vilkårene i databehandleraftalen og databeskyttelsesreglerne.
- Myndighederne har for 24 % af systemerne ikke haft kendskab til alle de underdatabehandlere, der har behandlet deres følsomme og fortrolige persondata.
- Justitsministeriet har ikke udgivet hverken en bekendtgørelse eller en vejledning om lokationskravet, som bestemmer, hvilke it-systemer der af hensyn til statens sikkerhed skal opbevares i Danmark.
- Væsentlige vejledninger fra Justitsministeriet og Finansministeriet udkom først, efter at myndighederne skulle have implementeret GDPR (databeskyttelsesforordningen).
- Datatilsynet har ikke ført et risikobaseret tilsyn og har ikke opdateret sin strategi, siden GDPR blev gældende i maj 2018. Datatilsynet har heller ikke gennemført de tilsyn hos offentlige myndigheder og private virksomheder, som var planlagt. Det har medført lav risiko for at blive opdaget i overtrædelser af reglerne om databeskyttelse.

Statsrevisorerne finder det bekymrende, at der stadig er så store problemer med sikring af følsomme og fortrolige persondata. Der er gået 8 år siden det største læk af fortrolige persondata og mere end 5 år, siden Statsrevisorerne skarpt kritiserede, at en række statslige institutioner ikke i tilstrækkeligt omfang beskytter fortrolige oplysninger om personer og virksomheder i *beretning nr. 1/2014 om statens behandling af fortrolige oplysninger om personer og virksomheder*.

Indholdsfortegnelse

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

Rigsrevisionen har revideret regnskaberne efter § 2, stk. 1, nr. 1, jf. § 3 i rigsrevisorloven.

Rigsrevisionen har gennemgået regnskaberne efter § 4, stk. 1, nr. 1, jf. § 6 i rigsrevisorloven.

Beretningen vedrører Region Midtjylland og alle ministerområder med undtagelse af Udenrigsministeriet, dvs. finanslovens § 5 og § 7-29. På alle de omfattede ministerområder har der været udskiftning på ministerposten i undersøgelsesperioden 2016-2020. Rigsrevisionen har derfor valgt ikke at opliste alle ministre.

Beretningen har i udkast været forelagt de omfattede ministerier og Region Midtjylland, hvis bemærkninger er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. Formål og konklusion

1. Data om dig er under angreb. Personlige oplysninger om borgere er ifølge Center for Cybersikkerhed i høj kurs hos cyberkriminelle og har været det gennem flere år. Hvis borgeres data ender hos de forkerte, kan det fx medføre tab af omdømme, identitetstyveri eller afpresning, og hvis data går tabt, kan det betyde, at det offentlige ikke kan levere en ordentlig service til borgerne.

2. Danmark er et af de mest digitaliserede lande i verden. Et stort udbud af digitale tjenester gør livet nemmere for både borgere, virksomheder og myndigheder, fx i form af borger.dk, NemID og TastSelv på skat.dk. Digitaliseringen betyder, at de offentlige myndigheder indsamler og behandler en stor mængde oplysninger om borgerne. Mange af oplysningerne er af følsom eller fortrolig karakter, fx cpr-numre og oplysninger om sundhed, politisk overbevisning og strafbare forhold. Det kan derfor have store negative konsekvenser for såvel den enkelte borger som den offentlige forvaltning, hvis oplysningerne ender i de forkerte hænder eller går tabt.

3. Ifølge *Strategi for it-styring i staten* (2017) er Danmark blandt de lande i EU, som outsourcer den største andel af statslige it-systemer. Outsourcing giver på den ene side mulighed for billigere drift og bedre udnyttelse af ekspertise, men stiller på den anden side øgede krav til myndighedernes styring af databehandlere, der behandler data om borgerne.

Outsourcing
Outsourcing betyder, at en opgave, fx drift, vedligeholdelse og udvikling af it-tjenester, overlades til en ekstern leverandør. Det kan enten være en privat virksomhed eller en anden offentlig myndighed.

Et eksempel på outsourcing er Justitsministeriet, der har hyret en privat it-leverandør til at opbevare data fra Kriminalregisteret.

4. Reglerne om behandling af personoplysninger er forankret i databeskyttelsesforordningen (herefter GDPR), som EU vedtog i april 2016. GDPR har været gældende siden den 25. maj 2018 og afløste i Danmark persondataloven fra 2000, som implementerede EU's databeskyttelsesdirektiv i dansk lov. GDPR viderefører flere af reglerne om databeskyttelse fra persondataloven. Det gælder bl.a. krav om, at den dataansvarlige skal udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn med databehandlere.

GDPR indførte dog også nye regler på området. Det gælder fx kravet om at udpege en databeskyttelsesrådgiver og muligheden for at give betydelige bøder, hvis reglerne ikke bliver overholdt. De nye regler og muligheden for bøder har ført til en øget opmærksomhed om håndteringen af persondata både i det private og i den offentlige forvaltning.

GDPR
GDPR er forkortelsen for General Data Protection Regulation. Den danske oversættelse er databeskyttelsesforordningen.

5. Denne undersøgelse går på tværs af hele staten og inkluderer regionerne i form af Region Midtjylland som case. Vi har inkluderet en region, fordi regionerne håndterer store mængder helbredsoplysninger om borgerne.

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

6. Formålet med undersøgelsen er at vurdere, om myndighederne har ydet en tilfredsstillende indsats for at sikre, at outsourcede følsomme og fortrolige persondata om borgerne opbevares sikkert. Vi besvarer følgende spørgsmål i beretningen:

- Har myndighederne haft en tilfredsstillende styring af databehandlere, som opbevarer følsomme eller fortrolige persondata?
- Har Justitsministeriet, herunder Datatilsynet, og Finansministeriet i tilstrækkelig grad understøttet de øvrige myndigheders styring af databehandlere?

Rigsrevisionen har selv taget initiativ til undersøgelsen i februar 2019.

Hovedkonklusion

Myndighederne har samlet set ydet en utilfredsstillende indsats for at sikre, at outsourcede følsomme og fortrolige persondata om borgerne opbevares sikkert. Konsekvensen er en øget risiko for, at borgernes følsomme og fortrolige data kompromitteres.

Myndighederne har samlet set haft en meget utilfredsstillende styring af databehandlere, som opbevarer følsomme eller fortrolige persondata, for de it-systemer, som indgår i undersøgelsen. Dette er på trods af, at kravene om at udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn med databehandlere har været gældende siden 2000. Særligt Udlændinge- og Integrationsministeriet og Region Midtjylland har haft en kritisabel styring af databehandlere. Finansministeriet har overordnet set haft den bedste styring af databehandlere sammenlignet med de øvrige myndigheder

Myndighederne har ikke udarbejdet en risikovurdering for 58 % af deres it-systemer, inden de har indgået en databehandleraftale. Dermed har myndighederne for størstedelen af systemerne ikke haft et grundlag for at fastsætte passende sikkerhedsforanstaltninger i databehandleraftalerne og planlægge deres tilsyn. Det finder Rigsrevisionen kritisabelt. Rigsrevisionen finder det særligt uhensigtsmæssigt, at myndighederne kun har udarbejdet en risikovurdering i 6 ud af de 17 tilfælde, hvor de benytter globale cloud-udbydere til at opbevare persondata. Det skyldes, at myndighederne skal godkende cloud-udbydernes standardvilkår, der som udgangspunkt ikke kan tilpasses de enkelte myndigheders behov. Rigsrevisionen finder det desuden utilfredsstillende, at flere myndigheder ikke har haft fuld klarhed over indholdet af de standardvilkår, som de har accepteret, når de benytter globale cloud-udbydere til at opbevare persondata.

Myndighederne havde ikke indgået en databehandleraftale for 14 % af systemerne, selv om de havde outsourcet opbevaringen af følsomme eller fortrolige persondata. Myndighederne havde i disse tilfælde ikke et juridisk grundlag for at kunne bestemme, hvordan databehandleren må behandle deres persondata. For en tredjedel af disse systemer har myndighederne imidlertid indgået en databehandleraftale undervejs i Rigsrevisionens undersøgelse, selv om data var outsourcet inden.

Myndighederne har ikke ført tilsyn med deres databehandlere for 23 % af systemerne og har dermed ikke undersøgt, om databehandlerne faktisk overholder vilkårene i databehandleraftalen og databeskyttelsesreglerne. For 40 % af de tilsyn, der er udført, har myndighederne ikke kunnet dokumentere, at de har fulgt op på tilsynenes resultater og taget stilling til, om de skal reagere over for databehandleren. Disse tilsyn har dermed ikke har tjent deres formål.

Manglende tilsyn kan have den konsekvens, at myndigheden ikke ved, om behandlingen af data sker inden for databehandleraftalens og databeskyttelsesreglernes rammer. Rigsrevisionens undersøgelse viser, at myndighederne ikke har haft kendskab til alle underdatabehandlere for 24 % af de systemer, hvor der benyttes underdatabehandlere. Det betyder, at underdatabehandlere i praksis har behandlet følsomme eller fortrolige persondata uden myndighedernes forudgående viden.

Justitsministeriet, herunder Datatilsynet, og Finansministeriet har ikke i tilstrækkelig grad understøttet de øvrige myndigheders styring af databehandlere
Justitsministeriet, Datatilsynet og Finansministeriet har udgivet 20 vejledninger, som de vurderede var nødvendige for at understøtte myndighederne i deres implementering af GDPR. Det finder Rigsrevisionen positivt.

Rigsrevisionen finder det imidlertid uhensigtsmæssigt, at 8 vejledninger først udkom, efter at myndighederne skulle have implementeret GDPR. Væsentlige vejledninger om udarbejdelsen af risikovurderinger og brugen af cloud-services udkom først mere end 1 år efter, at GDPR blev gældende. Desuden finder Rigsrevisionen det utilfredsstillende, at Justitsministeriet endnu ikke har udgivet hverken en bekendtgørelse eller en vejledning om lokationskravet (tidligere krigsreglen), som bestemmer, hvilke it-systemer der af hensyn til statens sikkerhed skal opbevares i Danmark.

Datatilsynet har ikke ført et risikobaseret tilsyn. Datatilsynet har ikke udarbejdet risikoanalyser til at understøtte planlægningen af sit tilsyn og har ikke opdateret sin strategi, siden GDPR blev gældende i maj 2018. Datatilsynet har ikke kunnet dokumentere, at de tilsyn, som Datatilsynet har planlagt, er udvalgt på baggrund af en risikobetragtning. Det betyder, at det er usikkert, om Datatilsynet har anvendt de tilgængelige ressurser til at føre tilsyn, der hvor risikoen er størst.

Datatilsynet har kun afsluttet 8 tilsyn med offentlige myndigheder og 14 tilsyn med private virksomheder, siden GDPR blev gældende. Det betyder, at der har været få afgørelser, som myndighederne kan bruge som fortolkningsbidrag i arbejdet med at sikre en tilstrækkelig styring af databehandlere og en korrekt implementering af GDPR. Det betyder også, at risikoen for at blive opdaget i overtrædelser af GDPR – og dermed tilsynenes præventive effekt – har været relativt lav.

1.2. Baggrund

7. Offentlige myndigheder indsamler og behandler data om landets borgere, når de skal forvalte deres opgaver og sikre en effektiv service. Hvor informationer om borgere tidligere blev opbevaret i arkivskabe og mapper, er data om borgere nu primært digitale og opbevares på servere og i datacentre.

8. Der er flere eksempler på, at borgernes oplysninger er blevet kompromitteret, når offentlige myndigheder har outsourcet oplysningerne til eksterne databehandlere. I 2012 fik hackere adgang til følsomme personoplysninger fra Rigspolitiet, SKAT, CPR-kontoret og Moderniseringsstyrelsen ved at hacke myndighedernes databehandler CSC. Roskilde Kommune mistede i 2018 over 80.000 dokumenter fra sit sundheds- og omsorgssystem, fordi kommunens databehandler KMD benyttede en underdatabehandler i Indien, som havde et servernedbrud, og en teknisk fejl fra KMD's side gjorde, at den relevante backup ikke var blevet foretaget korrekt. Samtidig har Center for Cybersikkerhed hvert år i perioden 2016-2019 vurderet truslen for cyberkriminalitet og cyberspionage mod Danmark til at være meget høj.

9. Datatilsynet har i flere tilfælde, inden GDPR blev gældende, konstateret problemer med, at offentlige myndigheder enten ikke har indgået databehandleraftaler eller ikke har ført tilsyn med, om databehandleraftalerne er blevet overholdt. Rigsrevisionen har desuden i en beretning fra 2016 om styring af it-sikkerheden hos it-leverandører kritiseret, at nogle offentlige myndigheder ikke har udarbejdet risikovurderinger, eller at risikovurderingerne ikke har været tilstrækkelige, når myndighederne outsourcede it-drift til eksterne it-leverandører.

10. Det har siden 2016 været et krav for statslige myndigheder, at de skal overholde sikkerhedsstandarden ISO 27001, mens regionerne har været forpligtede til at arbejde efter principperne i ISO 27001. ISO 27001 er en international standard for styring af informationssikkerhed, som skal understøtte myndighederne i at beskytte værdifulde informationer, herunder personoplysninger. Standarden forpligter bl.a. de statslige myndigheder til at sikre, at leverandører opretholder det aftalte niveau af informationssikkerhed. Digitaliseringsstyrelsen følger halvårligt op på, hvor langt de statslige myndigheder er med at implementere ISO 27001. En selvevaluering blandt statslige myndigheder i 2019 viste, at 37 % af de statslige myndigheder stadig ikke har et tilstrækkeligt modenhedsniveau for leverandørstyring.

Informationssikkerhed
Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer mod at gå tabt eller falde i forkerte hænder. I arbejdet indgår bl.a. organisering af sikkerhedsarbejdet, processer for behandling af data, styring af leverandører og tekniske sikkerhedsforanstaltninger.

11. Samlet set giver det et billede af, at offentlige myndigheder i flere tilfælde ikke har haft en tilstrækkelig styring af databehandlere.

Dataansvarlig, databehandler og underdatabehandler

12. Når offentlige myndigheder indsamler personoplysninger, bliver de dataansvarlige. Som dataansvarlig har myndighederne ansvaret for, at personoplysninger behandles sikkert. Opbevaring og behandling af personoplysninger kræver den nødvendige it-infrastruktur og ekspertise. Derfor kan det være hensigtsmæssigt for myndighederne – både sikkerhedsmæssigt og økonomisk – at outsource opbevaringen eller andre behandlinger af personoplysninger til private virksomheder eller specialiserede myndigheder, fx Statens It.

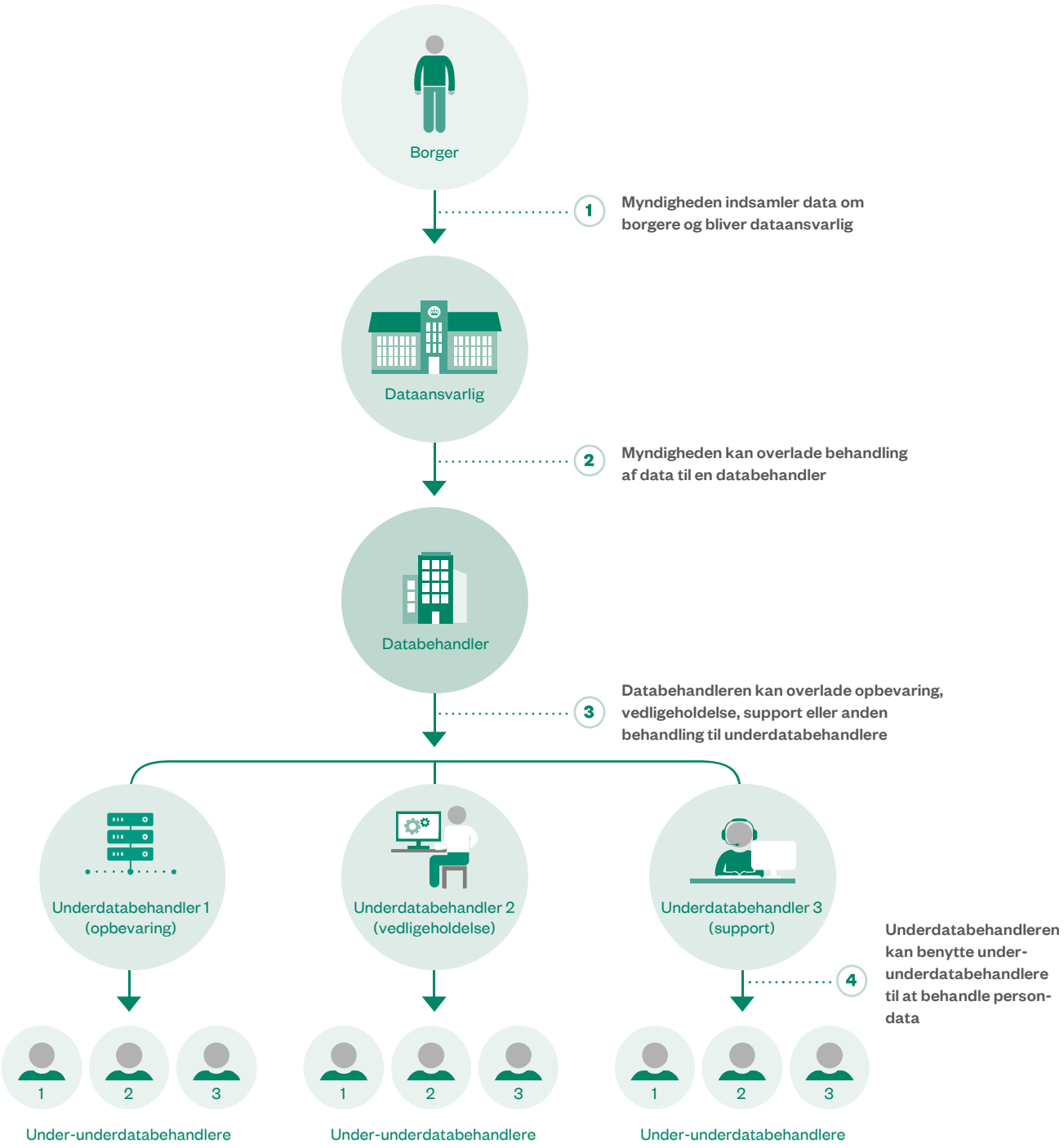
Dataansvarlig
En dataansvarlig er den juridiske eller fysiske person, private virksomhed, offentlige myndighed mv., der bestemmer, til hvilket formål og hvordan personoplysningerne må behandles.

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.

Hvis en offentlig myndighed outsourcer opbevaringen eller en anden behandling af personoplysninger til fx en privat virksomhed, indgår de i en databehandlerrelation, hvor den offentlige myndighed er dataansvarlig, og den private virksomhed er databehandler. Selv om data opbevares af en databehandler, er det stadig den dataansvarlige, der er ansvarlig for at sikre, at databehandleren stiller de fornødne garantier for, at der gennemføres de rette sikkerhedsmæssige foranstaltninger for opbevaringen af data. Det er også alene den dataansvarlige, der beslutter, hvordan databehandleren må behandle data og til hvilke formål.

En databehandler kan anvende underdatabehandlere til at varetage dele af sin databehandling. Det kan fx være at stille den serverplads til rådighed, hvor personoplysningerne opbevares. Det kan også være vedligeholdelse af databehandlerens it-infrastruktur eller support, hvis behandling af data er en central del af opgaven. Underdatabehandlere kan også selv anvende underdatabehandlere. Der kan derfor opstå databehandlerkæder, hvor det kan være svært for den dataansvarlige at bevare et samlet overblik. Figur 1 viser et eksempel på en databehandlerkæde.

Figur 1
Eksempel på en databehandlerkæde



Kilde: Rigsrevisionen.

Regler om databeskyttelse

13. Reglerne for behandling af personoplysninger er forankret i GDPR, som offentlige myndigheder og private virksomheder har skullet overholde siden den 25. maj 2018. GDPR suppleres i Danmark af databeskyttelsesloven, som dog ikke fastsætter andre regler på de undersøgte områder. Retshåndhævende myndigheders (fx politiet og domstolene) behandling af personoplysninger er reguleret i retshåndhævelsesloven, som trådte i kraft i april 2017. Reglerne i retshåndhævelsesloven er imidlertid i overensstemmelse med reglerne i GDPR på de punkter, som indgår i denne undersøgelse. Derfor er reglerne i GDPR udgangspunktet for undersøgelsen.

14. Vi har i undersøgelsen fokus på myndighedernes risikovurderinger, databehandleraftaler og tilsyn. Vi fokuserer på netop disse 3 elementer, da de dækker hele forløbet for outsourcing af persondata, dvs. før, under og efter, at databehandlingen er overladt til databehandleren.

15. I GDPR er omdrejningspunktet en risikobaseret tilgang til beskyttelse af persondata. Det betyder, at den dataansvarlige – allerede inden en behandling af persondata påbegyndes, eller persondata outsources – skal overveje de risici, der kan forekomme ved behandlingen. Overvejelserne skal ligge til grund for, hvilket sikkerhedsniveau der er nødvendigt, og hvilke forholdsregler der skal tages for at imødegå de identificerede risici – hverken mere eller mindre. Dette sker i form af en risikovurdering.

Resultatet af risikovurderingen skal i første omgang ligge til grund for beslutningen om, hvorvidt persondata i det hele taget skal outsources. Hvis persondata outsources, skal risikovurderingen ligge til grund for valget af sikkerhedsforanstaltninger i databehandleraftalen og være styrende for formen og hyppigheden af tilsynet med databehandleren. Dette er illustreret i figur 2. Hvis der fx er tale om et outsourcet it-system, som indeholder få ikke-følsomme personoplysninger, bør både sikkerhedskravene i databehandleraftalen og tilsynet være af mindre omfang. Hvis der omvendt outsources følsomme oplysninger om mange borgeres helbred, bør myndigheden sikre tilsvarende højere sikkerhedskrav i databehandleraftalen og føre et mere omfattende og hyppigere tilsyn med databehandleren.

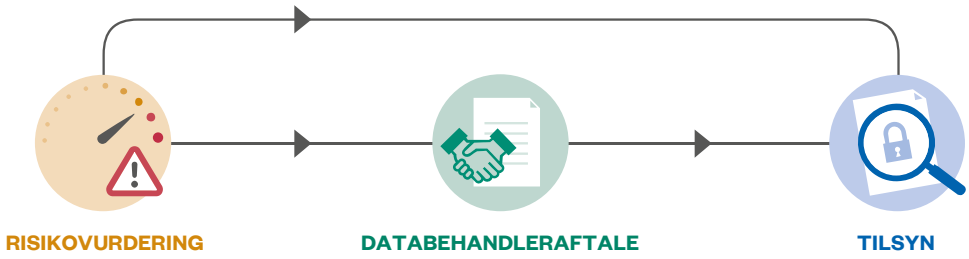
Databeskyttelsesloven
Databeskyttelsesloven (lov nr. 502 af 23. maj 2018) trådte i kraft samtidig med GDPR (25. maj 2018) og supplerer GDPR i en dansk kontekst.

Databeskyttelsesloven indeholder bl.a. en bestemmelse om, hvilke systemer der *skal* opbevares i Danmark (lokationskravet), og fastsætter nærmere regler for Datatilsynets arbejde.

Retshåndhævelsesloven
Retshåndhævelsesloven (lov nr. 410 af 27. april 2017) trådte i kraft den 27. april 2017.

Retshåndhævelsesloven gælder for retshåndhævende myndigheders (politi, anklagemyndighed, Kriminalforsorgen, Den Uafhængige Politianklagemyndighed og domstolene) behandling af personoplysninger på det strafferetlige område og træder i stedet for GDPR og databeskyttelsesloven. Mange af kravene i retshåndhævelsesloven er imidlertid sammenfaldende med reglerne i GDPR, herunder reglerne om risikovurderinger, databehandleraftaler og tilsyn.

Figur 2
Relationen mellem risikovurdering, databehandleraftale og tilsyn



Kilde: Rigsrevisionen.

16. GDPR's regler om risikovurderinger, databehandleraftaler og tilsyn er i store træk en videreførelse af persondatalovens regler på området, som har været gældende siden 2000. Det er derfor ikke nyt, at myndighederne skal udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn.

Figur 3 viser en sammenfatning af reglerne om risikovurderinger, databehandleraftaler og tilsyn før og efter, at GDPR blev gældende. Det fremgår af figuren, at det også var et krav i persondataloven, at der skulle udarbejdes risikovurderinger. Kravet blev imidlertid mere eksplicit med GDPR. Desuden blev det tydeliggjort, at risikovurderingerne skal tage udgangspunkt i risici for de registreredes rettigheder og ikke blot i risici for myndighedens egen forretning. Med GDPR blev der samtidig indført en række minimumskrav til indholdet af en databehandleraftale. Det gælder fx, at det skal fremgå af databehandleraftalen, at eventuelle underdatabehandlere skal overholde de samme krav som databehandleren. Endelig skal den dataansvarlige også under GDPR leve op til kravet om ansvarlighed og kunne påvise, at behandlingen af personoplysninger er i overensstemmelse med databeskyttelsesreglerne. Det betyder ifølge Datatilsynet, at den dataansvarlige skal føre tilsyn med sine databehandlere.

Figur 3
Regler om risikovurderinger, databehandleraftaler og tilsyn før og efter GDPR

	Persondataloven	GDPR Databeskyttelsesloven
DATABESKYTTELSESREGLER		
RISIKOVURDERING	• Den dataansvarlige skal træffe de fornødne sikkerhedsforanstaltninger for behandlingen af personoplysninger og dermed udarbejde en risikovurdering. *§ 41, stk. 3, i persondataloven*	• Det fremgår mere eksplicit, at den dataansvarlige skal risikovurdere behandlingen af personoplysninger for at afgøre, hvilke foranstaltninger der skal iværksættes. • Det er tydeliggjort, at risikovurderingen skal tage udgangspunkt i risici for de registreredes rettigheder. *Artikel 24, 25 og 32 mfl. i GDPR*
DATABEHANDLERAFTALE	• Den dataansvarlige skal indgå en databehandleraftale med sin databehandler. *§ 42, stk. 2, i persondataloven*	• Den dataansvarlige skal indgå en databehandleraftale med sin databehandler. • Der er en række minimumskrav for indholdet af en databehandleraftale. *Artikel 28 i GDPR*
TILSYN	• Den dataansvarlige skal påse behandlingssikkerheden hos databehandleren. *§ 42, stk. 1, i persondataloven*	• Den dataansvarlige skal påvise overholdelsen af databeskyttelsesreglerne. *Artikel 24 i GDPR*

Kilde: Rigsrevisionen.

1.3. Revisionskriterier, metode og afgrænsning

Revisionskriterier

17. Formålet med undersøgelsen er at vurdere, om myndighederne har ydet en tilfredsstillende indsats for at sikre, at outsourcede følsomme og fortrolige persondata om borgerne opbevares sikkert. Undersøgelsen inkluderer regionerne i form af Region Midtjylland som case. Region Midtjylland adskiller sig ikke umiddelbart fra de andre regioner på parametre som typen af følsomme og fortrolige persondata, typer af databehandlinger o.l. Vi har inkluderet en region, fordi regionerne håndterer store mængder følsomme personoplysninger fra sundhedssektoren.

18. I *kapitel 2* undersøger vi, om myndighederne har haft en tilfredsstillende styring af databehandlere, som opbevarer følsomme eller fortrolige persondata. Vi undersøger dermed ikke, om myndighederne generelt set overholder reglerne i GPDR, eller om it-sikkerheden i praksis er tilstrækkelig hos databehandlerne.

Vi undersøger for det første, om myndighederne har udarbejdet en risikovurdering, når de outsourcer opbevaringen af følsomme eller fortrolige personoplysninger. For det andet undersøger vi, om myndighederne har indgået databehandleraftaler med deres databehandlere, som opbevarer følsomme eller fortrolige persondata. For det tredje undersøger vi, om myndighederne har ført tilsyn med deres databehandlere, herunder om de har haft kendskab til de underdatabehandlere, der behandler deres følsomme eller fortrolige personoplysninger. Størstedelen af kriterierne tager udgangspunkt i de gældende regler under GDPR og databeskyttelsesloven, som alle myndigheder er forpligtede til at overholde, uanset hvornår de har taget deres it-systemer i brug, eller hvornår systemerne er outsourcet. Disse kriterier suppleres af kriterier, som baserer sig på Datatilsynets vejledninger og Rigsrevisionens opfattelse af, hvad en hensigtsmæssig styring af databehandlere indebærer. Baggrunden for de enkelte kriterier er beskrevet i de enkelte afsnit.

19. I *kapitel 3* undersøger vi, om Justitsministeriet, herunder Datatilsynet, og Finansministeriet i tilstrækkelig grad har understøttet de øvrige myndigheders styring af databehandlere.

Vi undersøger for det første, om de 3 myndigheder rettidigt har vejledt de øvrige myndigheder i forbindelse med implementeringen af GDPR. For det andet undersøger vi, om Datatilsynet har ført et risikobaseret tilsyn.

20. Det er til enhver tid de enkelte myndigheders ansvar at overholde gældende lovgivning, herunder GDPR. Ikke desto mindre kan de myndigheder, som har en central rolle på området og dermed den største ekspertise, understøtte de øvrige myndigheder i at overholde databeskyttelsesreglerne. En god understøttelse kan medvirke til, at myndighederne er bedre rustede til at overholde de gældende regler.

21. Justitsministeriet, herunder Datatilsynet, og Finansministeriet har alle centrale roller, hvad angår datasikkerhed, herunder styring af databehandlere. Justitsministeriet har ressortansvaret for GDPR og databeskyttelsesloven. Justitsministeriet har dermed mulighed for at vejlede myndighederne om lovgivningen, hvis der viser sig et behov for det.

Følsomme personoplysninger
Følsomme personoplysninger er ifølge GDPR oplysninger om race og etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetisk og biometrisk data, helbred og seksuel orientering. Behandling af disse personoplysninger kræver en højere grad af beskyttelse end almindelige personoplysninger.

Fortrolige personoplysninger
Fortrolige personoplysninger er ifølge databeskyttelsesloven cpr-numre og oplysninger om strafbare forhold. Strafbare forhold kan fx være oplysninger om lovovertrædelser og politianmeldelser.

Datatilsynet er den uafhængige tilsynsmyndighed på databeskyttelsesområdet. Datatilsynet skal på den ene side føre tilsyn med og håndhæve, at databeskyttelsesreglerne overholdes, og på den anden side rådgive og vejlede offentlige myndigheder og private virksomheder om databeskyttelsesreglerne. Det kan fx være ved at udgive vejledende tekster og offentliggøre afgørelser på baggrund af gennemførte tilsyn. Derudover har Datatilsynet også en række andre opgaver, fx at fremme offentlighedens kendskab til databeskyttelsesreglerne og deltage i internationalt samarbejde.

Digitaliseringsstyrelsen under Finansministeriet har til opgave at udforme og implementere digitaliseringsinitiativer i det offentlige. Som en del af den opgave skal Digitaliseringsstyrelsen understøtte en tilstrækkelig informationssikkerhed i den offentlige sektor, hvilket i mange tilfælde har snitflader til databeskyttelsesreglerne.

Metode

22. Undersøgelsens *kapitel 2* er baseret på en gennemgang af dokumentation for 148 it-systemer på tværs af staten og Region Midtjylland, hvor myndighederne har outsourcet opbevaringen af følsomme eller fortrolige personoplysninger til en databehandler. Vi har valgt at fokusere på systemer med følsomme og/eller fortrolige personoplysninger, idet en kompromittering af disse typer data kan have de største konsekvenser for borgerne. 108 ud af de 148 systemer indeholder følsomme personoplysninger, og de resterende 40 systemer indeholder fortrolige personoplysninger. 101 ud af de 148 systemer indeholder både følsomme og fortrolige personoplysninger. Vi har for alle systemerne gennemgået dokumentation for risikovurderinger, databehandleraftaler og tilsynsaktiviteter.

Behandling af personoplysninger
Behandling af personoplysninger er et bredt begreb, som fx kan omfatte opbevaring, indsamling, registrering, organisering, systematisering, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse af personoplysninger.

23. Behandling af personoplysninger kan have mange former. Vi fokuserer i kapitel 2 kun på outsourcing til databehandlere, som *opbevarer* persondata. Det gør vi ud fra en risikobetragtning, fordi databehandlere, som opbevarer data, typisk også foretager anden behandling af data, fx søgning i eller organisering af data. Desuden anvender databehandlere, som opbevarer data, i mange tilfælde underdatabehandlere til fx at vedligeholde servere eller yde support.

24. Vi har udvalgt de 148 it-systemer på baggrund af en bruttoliste på ca. 950 systemer, som ifølge myndighederne falder inden for undersøgelsens afgrænsning. Vi har udvalgt op til 10 systemer pr. myndighed, men færre i de tilfælde, hvor myndigheden ikke har haft 10 systemer, der falder inden for undersøgelsens afgrænsning. Vi har udvalgt systemerne ud fra en risikobetragtning på baggrund af oplysninger fra myndighederne om systemerne. Undersøgelsens resultater kan derfor ikke generaliseres til alle outsourcede it-systemer i staten og regionerne, som opbevarer følsomme eller fortrolige personoplysninger. De udvalgte systemer omfatter imidlertid en væsentlig andel af populationen.

25. Undersøgelsens *kapitel 3* bygger på:

- gennemgang af skriftligt materiale fra Finansministeriet, Justitsministeriet og Datatilsynet, herunder vejledninger, mødereferater, notater og strategipapirer
- data om Datatilsynets tilsynsaktivitet
- redegørelser fra Finansministeriet, Justitsministeriet og Datatilsynet
- en spørgeskemaundersøgelse, som omfatter alle statslige myndigheder, der har outsourcet opbevaringen af følsomme eller fortrolige persondata, og Region Midtjylland.

26. Vores metodiske tilgang, udvælgelse af it-systemer og operationalisering af kriterier er uddybet i bilag 1. I bilaget fremgår også en liste over de 148 it-systemer, som indgår i undersøgelsen, og vores kodebog, der uddyber, på hvilket grundlag vi har vurderet dokumentationen for de enkelte systemer.

27. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 1.

Afgrænsning

28. Undersøgelsen omfatter alle ministerier på nær Udenrigsministeriet, som har oplyst, at ministeriet ikke har outsourcet opbevaringen af følsomme eller fortrolige persondata. Vi har i udvælgelsen af myndigheder lagt vægt på også at dække det regionale niveau, som behandler mange følsomme helbredsoplysninger om borgere. Vi har på den baggrund udvalgt Region Midtjylland som case for regionerne. Undersøgelsen omfatter således 17 ministerier og én region.

29. Vi har i undersøgelsen afgrænset outsourcing til at omfatte tilfælde, hvor den dataansvarlige myndighed benytter en databehandler uden for ministeriets koncern. I undersøgelsen opfattes data således ikke som outsourcede, hvis fx en styrelse er databehandler for sit departement eller andre styrelser inden for samme koncern, medmindre data i sidste ende outsources ud af koncernen. En undtagelse er Statens It, som vi betragter som en ekstern databehandler for alle ministerier, selv om Statens It organisatorisk er en del af Finansministeriets koncern.

30. Vi foretager ikke en juridisk vurdering af, om risikovurderinger, databehandleraftaler og tilsyn i sin helhed lever op til alle regler i GDPR. Vi undersøger heller ikke, om fx databehandleraftalen i tilstrækkelig grad tager højde for de risici, som er identificeret i risikovurderingen, eller om de gennemførte tilsyn har været tilstrækkelige. Undersøgelsens sigte er derimod at se bredt på tværs af mange myndigheder og vurdere, om myndighederne overholder en række minimumskrav for styring af databehandlere.

31. Undersøgelsesperioden går fra GDPR's vedtagelse i EU i april 2016 til 1. januar 2020, hvor vi afsluttede vores materialeindsamling. Vi har kun inkluderet dokumentation for risikovurderinger og databehandleraftaler for de enkelte it-systemer, som er udarbejdet inden den 20. september 2019, hvor vi første gang modtog dokumentation fra myndighederne. Vi har kun inkluderet dokumentation for tilsynsaktiviteter, som er udarbejdet inden den 20. august 2019, hvor vi anmodede myndighederne om dokumentation for de enkelte systemer. Skæringsdatoerne er fastsat med henblik på at give et retvisende øjebliksbillede af de undersøgte myndigheders styring af databehandlere. Flere myndigheder har oplyst, at de efterfølgende har udarbejdet risikovurderinger, indgået databehandleraftaler, udført tilsyn eller fx skiftet databehandler for ét eller flere af deres systemer.

32. I bilag 1 er undersøgelsens metodiske tilgang beskrevet. Bilag 2 indeholder en ordliste, der forklarer udvalgte ord og begreber.

2. Myndighedernes styring af databehandlere

Delkonklusion

Myndighederne har samlet set haft en meget utilfredsstillende styring af databehandlere, som opbevarer følsomme eller fortrolige persondata, for de it-systemer, som indgår i undersøgelsen. Dette er på trods af, at kravene om at udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn med databehandlere har været gældende siden 2000. Særligt Udlændinge- og Integrationsministeriet og Region Midtjylland har haft en kritisabel styring af databehandlere. Finansministeriet har overordnet set har haft den bedste styring af databehandlere sammenlignet med de øvrige myndigheder.

For det første har myndighederne ikke udarbejdet en risikovurdering for 58 % af deres it-systemer, inden de indgik en databehandleraftale. I de tilfælde har myndighederne ikke haft et grundlag for at fastsætte passende sikkerhedsforanstaltninger i databehandleraftalerne og planlægge deres tilsyn. Rigsrevisionen finder dette kritisabelt. Myndighederne har for kun 18 % af systemerne udarbejdet en risikovurdering, inden de indgik en databehandleraftale, som også forholder sig til risici for de registreredes rettigheder og indeholder overvejelser om sandsynligheden for og konsekvensen ved, at der sker en sikkerhedshændelse. Rigsrevisionen finder det særligt uhensigtsmæssigt, at myndighederne kun har udarbejdet en risikovurdering for 6 ud af de 17 systemer, hvor data opbevares hos globale cloud-udbydere. Det skyldes, at myndighederne skal godkende cloud-udbydernes standardvilkår, der som udgangspunkt ikke kan tilpasses de enkelte myndigheders behov. Rigsrevisionen finder det desuden utilfredsstillende, at flere myndigheder ikke har haft fuld klarhed over indholdet af de standardvilkår, som de har accepteret, når de benytter globale cloud-udbydere til at opbevare persondata.

For det andet havde myndighederne for 14 % af de outsourcede systemer ikke et juridisk grundlag for at styre deres databehandlere, da de ikke havde en gældende databehandleraftale. For en tredjedel af disse systemer har myndighederne indgået en databehandleraftale undervejs i Rigsrevisionens undersøgelse, selv om data var outsourcet inden.

For det tredje har myndighederne ikke ført tilsyn med deres databehandlere for 23 % af systemerne. Dermed har de ikke undersøgt, om databehandleren overholder de aftalte vilkår. For 40 % af de udførte tilsyn har myndighederne ikke kunnet dokumentere, at de har fulgt op på tilsynenes resultater og taget stilling til, om de skal reagere over for databehandleren. Disse tilsyn har dermed ikke tjent deres formål.

Manglende tilsyn kan have den konsekvens, at myndigheden ikke ved, om behandlingen af data sker inden for databehandleraftalens og databeskyttelsesreglernes rammer. Undersøgelsen viser, at myndighederne ikke har haft kendskab til alle underdatabehandlere for 24 % af de systemer, hvor der benyttes underdatabehandlere. Det betyder, at underdatabehandlere i praksis har behandlet følsomme eller fortrolige persondata uden myndighedernes forudgående viden.

33. Dette kapitel handler om, hvorvidt myndighederne har haft en tilfredsstillende styring af databehandlere, som opbevarer følsomme eller fortrolige persondata. Vi undersøger myndighedernes arbejde med at udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn, herunder deres kendskab til underdatabehandlere.

2.1. Risikovurderinger

34. Vi har undersøgt, om myndighederne har udarbejdet en risikovurdering, inden de har indgået en databehandleraftale med databehandleren. Det har været et krav både under persondataloven og GDPR, at myndighederne skal udarbejde en risikovurdering, når de behandler personoplysninger. Formålet med en risikovurdering er bl.a. at vurdere, hvilke sikkerhedsforanstaltninger der skal skrives ind i databehandleraftalen, og hvilken form for tilsyn myndigheden skal gennemføre. Da risikovurderingen danner grundlag for, at myndighederne kan fastsætte de rette sikkerhedsforanstaltninger i databehandleraftalen, vurderer Rigsrevisionen, at det er vigtigt, at risikovurderingen er foretaget, inden databehandleraftalen indgås.

Vejledning om risikovurderinger
Datatilsynet har i samarbejde med Rådet for Digital Sikkerhed udgivet en vejledning om risikovurderinger.

Vejledningen indeholder bl.a. en risikovurderingsmetodik og en skabelon, som den dataansvarlige kan benytte i sit arbejde med risikovurderinger.

Vi har også undersøgt, om risikovurderingerne eksplicit forholder sig til risici for de registreredes rettigheder, fx hvilke konsekvenser det kan få for de registrerede, hvis deres data går tabt, eller uvedkommende får adgang til dem. Det fremgår af GDPR, at risikovurderingerne skal tage udgangspunkt i risici for de registreredes rettigheder. Det kan i praksis betyde, at it-systemer, som ikke er særligt kritiske på forretningsområdet, kan vise sig særligt risikofyldte for de registrerede og derfor også kræver særlige sikkerhedsforanstaltninger. Vi har ikke juridisk forholdt os til, om risikovurderingerne lever op til GDPR, men har ud fra en minimumsbetragtning vurderet, om risikovurderingerne eksplicit *forholder* sig til én eller flere risici for de registreredes rettigheder.

Endelig har vi undersøgt, om risikovurderingerne indeholder overvejelser om sandsynligheden for og konsekvensen ved mulige sikkerhedshændelser. Det fremgår af Datatilsynets vejledning om risikovurderinger, at risikovurderingen bør omfatte overvejelser om sandsynlighed og konsekvens, da det giver et samlet overblik over risikobilledet.

35. Figur 4 viser, om myndighederne har udarbejdet risikovurderinger for deres it-systemer, og om risikovurderingerne er udarbejdet, inden databehandleraftalen er indgået.

Figur 4
Risikovurderinger pr. myndighed og samlet

[1)] Denne kategori indeholder også enkelte tilfælde, hvor der er udarbejdet en risikovurdering, men hvor der ikke er indgået en databehandleraftale.

Note: n=148 it-systemer fordelt på alle 18 myndigheder.

Kilde: Rigsrevisionen.

Det fremgår af figur 4, at myndighederne for 42 % af it-systemerne ikke har foretaget en risikovurdering, selv om det er et lovkrav. For yderligere 16 % af systemerne har myndighederne først udarbejdet en risikovurdering, efter at databehandleraftalen er indgået. Risikovurderingen kan derfor ikke have ligget til grund for de krav, der blev skrevet ind i databehandleraftalen. Der kan dog være tilfælde, hvor myndighederne på baggrund af en senere risikovurdering har genbesøgt deres databehandleraftale og vurderet, at aftalen var tilstrækkelig. 11 ud af de 18 myndigheder har udarbejdet en risikovurdering for under halvdelen af deres systemer, inden de har indgået databehandleraftaler. Finansministeriet og Kulturministeriet skiller sig positivt ud i forhold til de øvrige myndigheder ved at have udarbejdet en risikovurdering for henholdsvis 9 ud af 10 systemer og 5 ud af 6 systemer, inden de har indgået en databehandleraftale.

Boks 1 beskriver et eksempel på et it-system, hvor der ikke er udarbejdet en risikovurdering.

Boks 1

Eksempel på manglende risikovurdering

Region Midtjylland bruger en privat databehandler til at sende elektroniske breve, fx henvisning til egen læge eller oplysninger til kommuner og andre eksterne parter. I den forbindelse sker der også en midlertidig opbevaring af data hos databehandleren. Systemet indeholder både følsomme og fortrolige personoplysninger. Region Midtjylland har ikke udarbejdet en risikovurdering for systemet, inden systemet blev outsourcet.

Det fremgår desuden af figur 4, at myndighederne for de resterende 42 % af it-systemerne har foretaget en risikovurdering, inden databehandleraftalen blev indgået. Af de 42 % forholder knap halvdelen sig ikke eksplicit til risici for de registreredes rettigheder, og en fjerdedel forholder sig ikke til sandsynligheden for og konsekvensen ved, at der indtræffer en hændelse, som kompromitterer datasikkerheden. Disse risikovurderinger udgør derved et svagere grundlag for den dataansvarlige til at kunne vurdere, hvilke sikkerhedsforanstaltninger databehandleraftalen bør indeholde for at opretholde et højt sikkerhedsniveau, ikke mindst for så vidt angår risici for de registreredes rettigheder.

Samlet set har myndighederne for kun 18 % af it-systemerne i undersøgelsen udarbejdet en risikovurdering, som opfylder alle de krav, vi har undersøgt. Dvs. at risikovurderingen er udarbejdet, inden myndigheden har indgået en databehandleraftale, og at den forholder sig til både risici for de registreredes rettigheder, som er et krav ifølge GDPR, og til sandsynligheden for og konsekvensen ved en sikkerhedshændelse.

36. Boks 2 giver et eksempel på en myndighed, der har arbejdet systematisk med at udarbejde risikovurderinger for sine it-systemer.

Boks 2

Eksempel på en systematisk tilgang til risikovurderinger

Statens Administration har en systematisk tilgang til arbejdet med risikovurderinger. Statens Administration udarbejder årligt en samlet risikovurdering for alle sine it-systemer, processer og leverandører. I risikovurderingen forholder Statens Administration sig til:

- Konsekvensen for de registreredes rettigheder, hvis der sker et sikkerhedsbrud, fx datalæk eller uautoriseret brug af personoplysninger.
- Det samlede risikobillede på baggrund af overvejelser om sandsynligheder og konsekvenser for sikkerhedsbrud.
- Hvilke tiltag der skal iværksættes for at styrke sikkerheden. Tiltagene beskrives i en kort handleplan for hvert system, som indeholder et tidspunkt for, hvornår tiltagene skal være iværksat.

Risikovurderinger ved brug af cloud-services

37. En række myndigheder gør brug af såkaldte cloud-services. Når man taler om outsourcing af persondata, vil cloud-services typisk dække over løsninger, hvor opbevaringen af data ikke foregår lokalt, men i ét eller flere eksterne datacentre. Cloud-services kan være fordelagtige, fordi de ofte er billigere, da løsningerne er fleksible og kun trækker på den kapacitet, som er nødvendig. Der er imidlertid nogle særlige karakteristika for cloud-services leveret af globale cloud-udbydere, som myndighederne skal være opmærksomme på. Det gælder fx, at myndighederne skal godkende cloud-udbydernes standardvilkår, som ikke kan tilpasses den enkelte myndigheds behov. Standardvilkårene indebærer, at myndighederne giver en generel godkendelse til, at udbyderne benytter underdatabehandlere i hele verden, som det i praksis kan være svært at føre tilsyn med. Det er derfor særligt vigtigt, at myndighederne foretager en risikovurdering, inden de gør brug af cloud-services hos en global cloud-udbyder.

38. Undersøgelsen viser, at myndighederne kun har udarbejdet en risikovurdering for 6 ud af de 17 it-systemer, hvor der benyttes globale cloud-udbydere, inden de har outsourcet opbevaringen af persondata.

Cloud-services

Cloud-services dækker bredt set over internetbaserede it-løsninger. Løsningerne kan have mange former – fra programmer som fx Gmail og Facebook, som tilgås via internettet og ikke er installeret på computeren, til løsninger, som kun opbevarer data. Opbevaringsløsningerne kan variere i fuldstændighed – fra færdige løsninger som fx Dropbox og Google Drive til mere rå serverkapacitet som fx Microsoft Azure og Amazon Web Service.

Fælles for løsningerne er, at data og applikation ligger på internettet og ikke på den computer, som man tilgår løsningerne fra.

Mere information om brugen af cloud findes i Digitaliseringsstyrelsens vejledning til anvendelse af cloud.

Resultater

Undersøgelsen viser, at myndighederne ikke har udarbejdet en risikovurdering for 42 % af it-systemerne, selv om det er et lovkrav. For yderligere 16 % af systemerne har myndighederne først udarbejdet en risikovurdering, efter de har indgået en databehandleraftale. Det betyder, at myndighederne for størstedelen (58 %) af systemerne, som opbevarer følsomme eller fortrolige persondata, ikke har haft et grundlag for at kunne fastsætte tilstrækkelige sikkerhedsforanstaltninger i databehandleraftalerne og til at kunne planlægge deres tilsyn. 11 ud af de 18 myndigheder har udarbejdet en risikovurdering for under halvdelen af deres systemer, inden de indgik en databehandleraftale. Finansministeriet har udarbejdet en risikovurdering for 9 ud af 10 systemer og Kulturministeriet for 5 ud af 6 systemer, inden de indgik en databehandleraftale.

Undersøgelsen viser også, at myndighederne har udarbejdet en risikovurdering for 42 % af systemerne, inden de indgik en databehandleraftale. Halvdelen af disse risikovurderinger forholder sig imidlertid ikke til risici for de registreredes rettigheder, og en fjerdedel indeholder ikke overvejelser om sandsynlighed og konsekvens. Samlet set har myndighederne kun udarbejdet en risikovurdering for 18 % af de undersøgte systemer, som opfylder alle de krav, vi har undersøgt. Dvs. at myndigheden har udarbejdet en risikovurdering, inden myndigheden har indgået en databehandleraftale, og at risikovurderingen forholder sig til både risici for de registreredes rettigheder, som er et krav ifølge GDPR, og til sandsynligheden for og konsekvensen ved, at der sker en sikkerhedshændelse.

Endelig viser undersøgelsen, at myndighederne kun har udarbejdet en risikovurdering for 6 ud af 17 systemer, hvor persondata opbevares hos en global cloud-udbyder. Det finder Rigsrevisionen særligt uhensigtsmæssigt, fordi der gør sig særlige forhold gældende ved brugen af globale cloud-udbydere, som myndighederne bør forholde sig til.

2.2. Databehandleraftaler

39. Vi har undersøgt, om myndighederne har indgået databehandleraftaler med deres databehandlere, som opbevarer følsomme eller fortrolige persondata. Vi har også undersøgt, om data fysisk opbevares inden for det aftalte område, som fremgår af databehandleraftalen.

Den dataansvarlige og databehandleren skal indgå en skriftlig databehandleraftale, når behandlingen af persondata overlades til databehandleren. Dette er et krav i GDPR og har været et udtrykkeligt lovkrav, siden persondataloven blev gældende i 2000. Databehandleraftalen er det juridiske grundlag, der regulerer, hvordan databehandleren må behandle personoplysningerne. Det kan fx være, om databehandleren skal have en specifik godkendelse af nye underdatabehandlere fra den dataansvarlige, hvorfra i verden data må behandles, eller om databehandleren skal slette personoplysningerne, når samarbejdet ophører.

40. Figur 5 viser, om myndighederne har indgået databehandleraftaler med deres databehandlere, som opbevarer følsomme eller fortrolige personoplysninger.

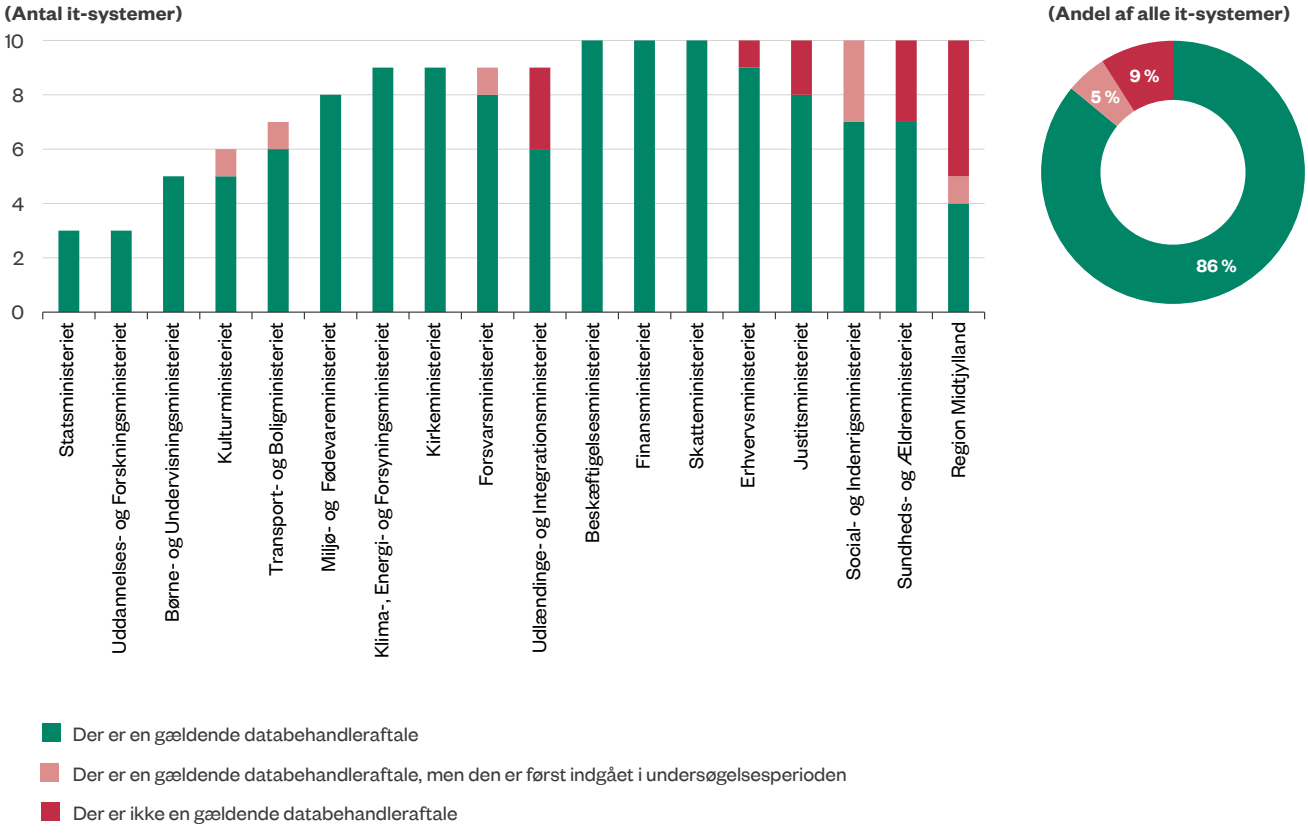
Vejledningsmateriale om databehandleraftaler

Datatilsynet har udgivet en vejledning om databehandlere og dataansvarlige.

Vejledningen beskriver, hvilke overvejelser den dataansvarlige bør gøre sig ved indgåelse af en databehandleraftale. Datatilsynet har også udarbejdet en standarddatabehandleraftale, som er en skabelon for, hvordan en databehandleraftale kan udformes.

Figur 5

Databehandleraftaler pr. myndighed og samlet



Note: n=148 it-systemer fordelt på alle 18 myndigheder. De 5 % af databehandleraftalerne, som er indgået i undersøgelsesperioden, er indgået i perioden, fra Rigsrevisionen påbegyndte sin hovedundersøgelse i juni 2019, til Rigsrevisionen afsluttede materialeindsamlingen for databehandleraftaler i september 2019.

Kilde: Rigsrevisionen.

Det fremgår af figur 5, at myndighederne samlet set havde indgået en databehandleraftale for 86 % af deres it-systemer, da vi påbegyndte undersøgelsen i juni 2019. 9 ud af de 18 myndigheder havde gældende databehandleraftaler for alle deres outsourcede systemer, da vi påbegyndte undersøgelsen. For 5 % af systemerne har myndighederne først indgået en databehandleraftale undervejs i Rigsrevisionens undersøgelse, selv om systemerne var outsourcet inden. Social- og Indenrigsministeriet, Forsvarsministeriet, Transport- og Boligministeriet og Kulturministeriet har undervejs i undersøgelsesperioden indgået nye databehandleraftaler, så ministerierne nu har databehandleraftaler for alle de systemer, der indgår i undersøgelsen. Myndighederne har ikke indgået en databehandleraftale for 9 % af deres outsourcede systemer med følsomme eller fortrolige personoplysninger. Region Midtjylland, Udlændinge- og Integrationsministeriet, Sundheds- og Ældreministeriet og Justitsministeriet har ikke en gældende databehandleraftale for flere af deres systemer.

41. Boks 3 giver 2 eksempler på it-systemer, hvor der ikke er indgået en databehandleraftale.

Boks 3

Eksempler på manglende databehandleraftaler

Sundhedsdatastyrelsen
Sundhedsdatastyrelsen opbevarer Organdonorregisteret hos en privat it-leverandør. Systemet indeholder cpr-numre om organdonorer. Sundhedsdatastyrelsen har ikke en databehandleraftale og har derfor ikke et juridisk grundlag til at styre, hvordan databehandleren anvender personoplysningerne.

Styrelsen for International Rekruttering og Integration
Styrelsen for International Rekruttering og Integration (SIRI) anvender en privat it-leverandør til at vurdere ægtheden af opholdsdokumenter, når udenlandske borgere søger om opholdstilladelse. Opholdsdokumenterne, fx udenlandske pas, indeholder typisk et nationalt id-nummer, som er en fortrolig oplysning. SIRI overtog systemet fra Statsforvaltningen ved ressortoverdragelse pr. 1. april 2019, hvor der ikke forelå en databehandleraftale. Arbejdet med at indgå en databehandleraftale er endnu ikke afsluttet. SIRI har derfor på nuværende tidspunkt ikke et juridisk grundlag, der bestemmer, hvordan databehandleren må anvende disse personoplysninger.

42. For 27 % af it-systemerne i undersøgelsen (40 systemer) er databehandleraftalen indgået, før GDPR blev gældende den 25. maj 2018. Vores gennemgang viser, at knap halvdelen (18) af databehandleraftalerne henviser til persondataloven og ikke til GDPR. Det indikerer, at databehandleraftalerne for 18 systemer, svarende til 12 % af systemerne i undersøgelsen, ikke fuldt ud lever op til kravene i GDPR.

Digital Post-løsningen

43. En række it-systemer er fællesstatslige og benyttes af mange myndigheder. For systemet Digital Post har flere myndigheder oplevet, at der er uklarhed om, hvem der har ansvaret for at udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn med e-Boks, som leverer løsningen. Digitaliseringsstyrelsen har oplyst, at de enkelte myndigheder er dataansvarlige for de personoplysninger, som de sender via Digital Post, og derfor er ansvarslige for selv at udarbejde en risikovurdering, indgå en databehandleraftale og føre et passende tilsyn. Dette var også tilfældet under persondataloven og er ikke blevet ændret som følge af GDPR. Digital Post indgår 7 gange i undersøgelsen, hvor 7 forskellige myndigheder er dataansvarlige. Undersøgelsen viser, at myndighederne i 2 ud af de 7 tilfælde ikke har indgået en databehandleraftale med e-Boks.

44. Digitaliseringsstyrelsen har tilkendegivet, at det ud fra en resursemæssig betragtning ikke er hensigtsmæssigt, at alle myndigheder selv er ansvarlige for at føre tilsyn med e-Boks. Det er imidlertid Digitaliseringsstyrelsens vurdering, at styrelsen ikke inden for de gældende juridiske rammer kan føre tilsyn på vegne af de enkelte dataansvarlige myndigheder. Digitaliseringsstyrelsen har i forbindelse med vores undersøgelse aftalt med e-Boks, at Digitaliseringsstyrelsens databehandleraftale og revisorerklæring gøres tilgængelige for øvrige myndigheder. Digitaliseringsstyrelsen vil også synliggøre, hvordan styrelsen fører tilsyn med e-Boks med henblik på, at de øvrige myndigheder kan vurdere, om Digitaliseringsstyrelsens tilsyn er tilstrækkeligt i forhold til myndighedernes egen risikovurdering.

Fællesstatslige it-systemer
Fællesstatslige it-systemer er systemer, som én myndighed er ansvarlig for, men som benyttes af en lang række myndigheder på tværs af staten, fx Statens Budgetsystem og statens rejseafregnings- og udlægssystem (RejsUd).

Typisk er den ansvarlige myndighed, og ikke de enkelte myndigheder, dataansvarlig for data, som behandles i fællesstatslige systemer.

Fysisk opbevaring af persondata

45. For at sikre, at EU's databeskyttelsesregler ikke udvandes, hvis data føres ud af EU, gælder der særlige regler, når persondata overføres til tredjelande eller internationale organisationer. Vi har undersøgt, om myndighederne har defineret, hvor databehandlerne må opbevare deres persondata, og bedt myndighederne indhente oplysninger fra deres databehandler om, hvor data faktisk blev opbevaret.

46. Myndighederne har for 85 % af it-systemerne i undersøgelsen (126 ud af 148 systemer) stillet krav til databehandleren om, at deres personoplysninger skal opbevares i Danmark eller inden for EU/EØS. For de resterende 15 % har myndighederne ikke taget stilling til, hvor deres data må opbevares.

Personoplysningerne i 123 ud af de 126 it-systemer blev ifølge databehandlerne opbevaret inden for det område, som myndigheden havde bestemt. I 2 tilfælde blev data opbevaret i et andet EU-/EØS-land, selv om det fremgik af databehandleraftalen, at data skulle opbevares i Danmark. Desuden kunne Beredskabsstyrelsen under Forsvarsministeriet ikke dokumentere, hvor data fra et af deres systemer fysisk blev opbevaret. Beredskabsstyrelsen har efterfølgende opsagt samarbejdet med databehandleren. Data for de 15 % af systemerne, hvor der ikke var taget stilling til opbevaring, blev i alle tilfælde ifølge databehandlerne opbevaret i Danmark eller i et andet EU-/EØS-land.

Tredjelande
Tredjelande er lande, som ikke er medlem af EU eller EØS (Island, Lichtenstein og Norge). Som udgangspunkt er alle lande uden for EU/EØS at betragte som usikre tredjelande. Europa-Kommissionen har imidlertid afgjort, at beskyttelsesniveauet for en række tredjelande lever op til sikkerhedsstandarderne, der gælder inden for EU, og dermed kan betragtes som sikre tredjelande. Det gælder fx Schweiz, New Zealand og organisationer/virksomheder i USA, som har tilsluttet sig EU-U.S. Privacy Shield.

Datatilsynet har udgivet en vejledning om overførsler til tredjelande. Vejledningen beskriver bl.a., hvad en dataansvarlig skal være opmærksom på ved overførsler til sikre og usikre tredjelande.

Standardvilkår ved brug af cloud-services

47. Når myndighederne bruger globale cloud-udbydere som databehandlere eller underdatabehandlere, består databehandleraftalen som udgangspunkt af cloud-udbyderens standardvilkår, som ikke kan tilpasses den enkelte myndigheds behov. Af standardvilkårene fremgår det typisk, at cloud-udbyderen har en generel godkendelse til at benytte underdatabehandlere, som kan være placeret rundt omkring i verden og i visse situationer kan tilgå persondata.

Vores undersøgelse viser, at flere myndigheder ikke har været klar over, at de har givet den globale cloud-udbyder generel godkendelse til at anvende underdatabehandlere fra sikre og usikre tredjelande, der som udgangspunkt kan få *adgang* til at behandle myndighedernes data, fx i forbindelse med support eller vedligeholdelse af servere.

Resultater

Undersøgelsen viser, at myndighederne ikke har indgået en databehandleraftale for 9 % af deres outsourcede it-systemer med følsomme eller fortrolige oplysninger, og at de for 5 % af systemerne først har indgået en databehandleraftale undervejs i Rigsrevisionens undersøgelse, selv om data var outsourcet inden. Dette er tilfældet, selv om lovkravet om databehandleraftaler har været gældende siden 2000. Region Midtjylland, Udlændinge- og Integrationsministeriet, Sundheds- og Ældreministeriet og Justitsministeriet skiller sig ud ved ikke at have indgået databehandleraftaler for flere af deres systemer. 9 ud af de 18 myndigheder havde indgået en databehandleraftale for alle deres systemer, da Rigsrevisionen påbegyndte undersøgelsen. Databehandleraftalerne for 12 % af systemerne i undersøgelsen er indgået inden GDPR og henviser til de gamle databeskyttelsesregler. Det indikerer, at de ikke fuldt ud lever op til de gældende databeskyttelsesregler i GDPR.

Undersøgelsen viser, at flere myndigheder har oplevet uklarhed om ansvarsfordelingen for systemet Digital Post, herunder hvem der skal føre tilsyn med databehandleren e-Boks. Det er Rigsrevisionens vurdering, at Digitaliseringsstyrelsen tidligere burde have stillet sit tilsyn til rådighed for de øvrige myndigheder, så myndighederne kunne vurdere, om det udførte tilsyn var tilstrækkeligt i forhold til deres egen risikovurdering.

Undersøgelsen viser desuden, at myndighederne for 85 % af systemerne i undersøgelsen har stillet krav om, hvor deres personoplysninger fysisk må opbevares. Rigsrevisionen kan konstatere, at data ifølge databehandlerne for alle undtagen 3 systemer var fysisk placeret i overensstemmelse med myndighedernes krav. I 2 tilfælde var data opbevaret i et andet EU-/EØS-land, selv om data skulle opbevares i Danmark. For et enkelt system har Beredskabsstyrelsen ikke kunnet oplyse, hvor data opbevares. Myndighederne har for 15 % af systemerne i undersøgelsen ikke taget stilling til, hvor data må opbevares. Her blev data ifølge databehandlerne i alle tilfælde opbevaret i Danmark eller i et andet EU-/EØS-land.

Endelig viser undersøgelsen, at flere myndigheder ikke har været klar over, at de har givet globale cloud-udbydere generel godkendelse til at anvende underdatabehandlere i sikre og usikre tredjelande, der som udgangspunkt kan få adgang til at behandle deres data. Myndighederne har således ikke har haft fuld klarhed over indholdet af de globale cloud-udbyderes standardvilkår, som de eller deres databehandlere har accepteret.

2.3. Tilsyn

48. Vi har undersøgt, om myndighederne har ført tilsyn med deres databehandlere. Det har vi gjort ved at undersøge, om myndighederne har en plan for at føre tilsyn med deres databehandlere, om myndighederne faktisk har ført tilsyn med deres databehandlere, og om myndighederne har fulgt op på de tilsyn, som de har gennemført.

Vejledningsmateriale om tilsyn
Datatilsynet har udgivet en vejledning, der bl.a. beskriver, hvordan man kan føre tilsyn med databehandlere og underdatabehandlere.

Vi har desuden undersøgt, om myndighederne har kendskab til alle underdatabehandlere, som behandler deres persondata, og om myndighederne har sikret, at der er ført tilsyn med underdatabehandlere.

49. Tilsyn skal sikre, at databehandlerne i praksis overholder de krav, som er fastsat i databehandleraftalerne og i de gældende databeskyttelsesregler. Det er ikke et lovkrav at have en tilsynsplan, men Rigsrevisionen vurderer, at en tilsynsplan sikrer, at myndighederne har overblik over og sikrer konsistens i de tilsyn, som myndighederne skal udføre. Det er Datatilsynets opfattelse, at kravet om at føre tilsyn følger af GDPR, idet den dataansvarlige skal kunne påvise, at behandlingen overholder GDPR og databehandleraftalen. Datatilsynet lægger vægt på, at formen og hyppigheden af tilsynet afhænger af den forudgående risikovurdering. Endelig er det Rigsrevisionens opfattelse, at værdien af et udført tilsyn først kommer til udtryk, når myndigheden følger op på tilsynets resultater, dvs. at myndigheden tager stilling til, om de skal reagere over for databehandleren på baggrund af tilsynets resultater.

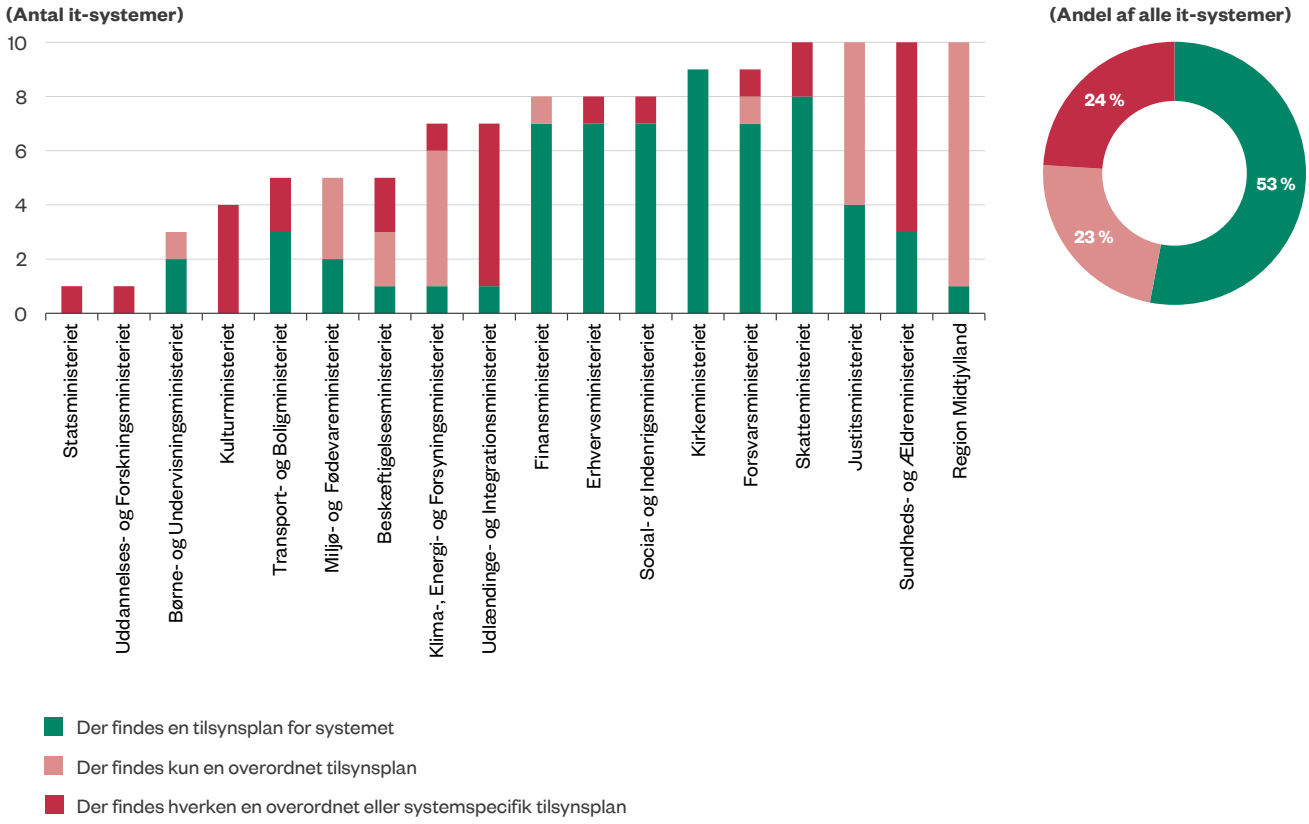
Det følger af GDPR, at en databehandler ikke må bruge underdatabehandlere, uden at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse. Ved specifik godkendelse må databehandleren ikke anvende underdatabehandlere, før den dataansvarlige specifikt har godkendt de konkrete underdatabehandlere. Hvis det fremgår af databehandleraftalen, at myndigheden har givet en generel godkendelse, skal myndigheden stadig orienteres om brugen af nye underdatabehandlere. Hvis myndigheden har et mangelfuldt tilsyn med sin databehandler, kan en konsekvens være, at myndigheden ikke har kendskab til alle underdatabehandlere, eller at databehandleren ikke fører tilsyn med underdatabehandlere.

Planer for tilsyn med databehandlere

50. Figur 6 viser, om myndighederne har en plan for at føre tilsyn med deres databehandlere. En tilsynsplan kan enten fremgå direkte af databehandleraftalen, hvor det fx bestemmes, at der skal indhentes en årlig revisorerklæring af en bestemt type, eller af en selvstændig tilsynsplan i myndigheden.

Figur 6

Planer for tilsyn med databehandlere pr. myndighed og samlet



Note: n=120 it-systemer fordelt på alle 18 myndigheder. Systemer, hvor Statens It eller Statens Administration er databehandler, fremgår ikke af figuren, da Finansministeriet har ansvaret for at føre tilsyn med disse systemer. En overordnet tilsynsplan skal forstås som en plan, der ikke forholder sig til det enkelte system. En overordnet tilsynsplan vil typisk omfatte fx en enkelt styrelse og vil oftest ikke gælde hele ministerområdet.

Kilde: Rigsrevisionen.

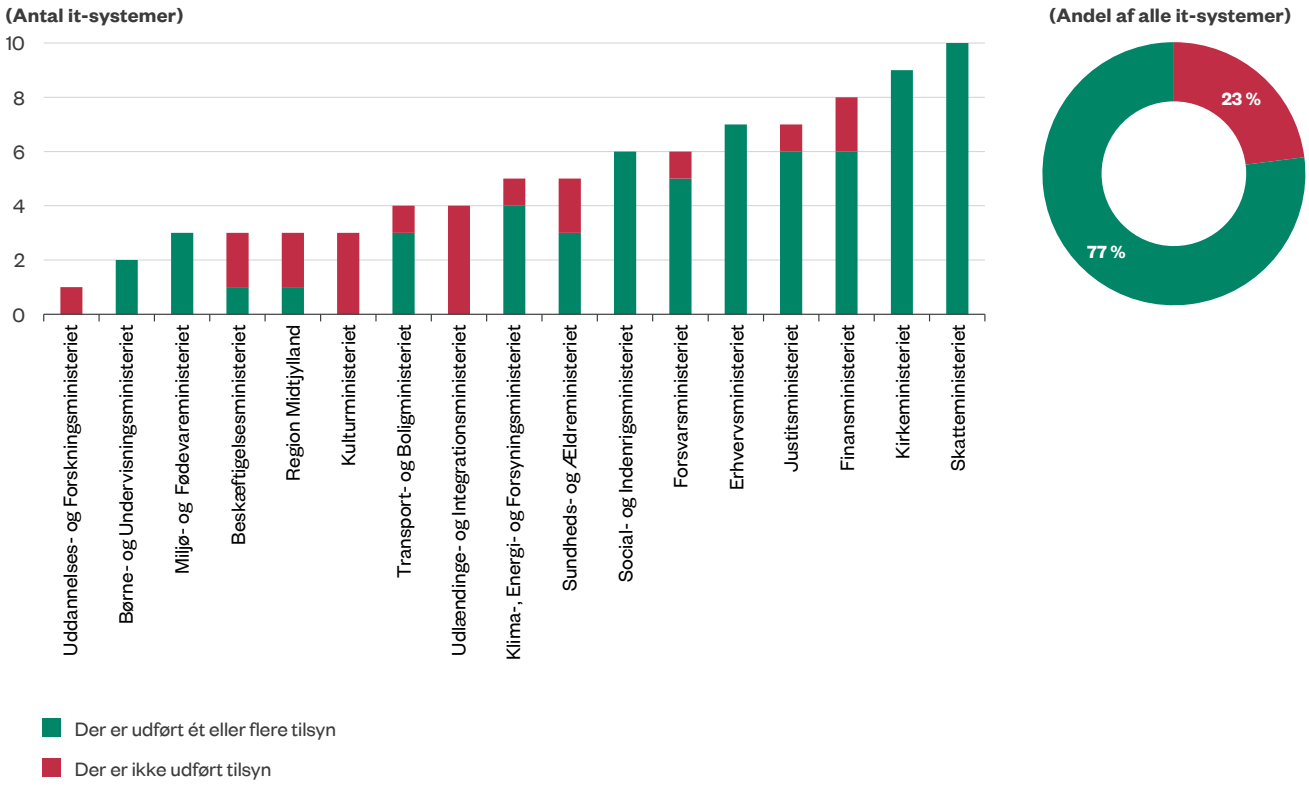
Det fremgår af figur 6, at myndighederne har en plan for at føre tilsyn med databehandlerne for 53 % af deres outsourcede it-systemer. Myndighederne har ikke en plan for at føre tilsyn for 24 % af deres systemer, og for 23 % af systemerne findes der kun en overordnet tilsynsplan. Det betyder, at myndigheden har et overordnet koncept for, hvordan der generelt skal føres tilsyn med myndighedens databehandlere, men at myndigheden ikke har bestemt, hvordan og hvor ofte der skal føres tilsyn med det specifikke system. 10 ud af de 18 myndigheder har en tilsynsplan for under halvdelen af deres systemer. Kirkeministeriet har som den eneste myndighed en tilsynsplan for alle sine systemer.

Tilsyn med databehandlere

51. Tilsyn med databehandlere kan have flere forskellige former og bør afspejle den risikovurdering, som myndigheden har foretaget. Et tilsyn kan enten ske ved, at myndigheden indhenter en specifik eller generel revisorerklæring, som udarbejdes af eksterne revisorer, eller ved, at myndigheden selv indhenter oplysninger eller gennemfører fysiske inspektioner hos databehandleren. Figur 7 viser, om myndighederne har ført tilsyn med deres databehandlere, hvor der er indgået en databehandleraftale.

Figur 7

Tilsyn med databehandlere pr. myndighed og samlet



Note: n=86 it-systemer fordelt på 17 myndigheder. I figuren indgår kun systemer, hvor der findes en databehandleraftale. Systemer, hvor der ikke er ført tilsyn, men hvor der er gået mindre end 1 år siden indgåelse af databehandleraftalen, indgår ikke. Desuden indgår systemer, hvor Statens It eller Statens Administration er databehandler, heller ikke, da Finansministeriet er ansvarlig for at føre tilsyn med disse systemer. Statsministeriet indgår ikke i opgørelsen, idet ingen af ministeriets systemer falder inden for disse afgrænsninger.

Kilde: Rigsrevisionen.

Generel revisorerklæring
En generel revisorerklæring omfatter som udgangspunkt databehandlerens generelle it-sikkerhed, interne kontroller og i nogle tilfælde databeskyttelse. Denne type erklæring omfatter som udgangspunkt ikke det specifikke system eller den behandling af persondata, som finder sted i systemet.

Specifik revisorerklæring
En specifik revisorerklæring omfatter det specifikke it-system eller den specifikke databehandling, som myndigheden har outsourcet.

Ny type revisorerklæring
FSR - danske revisorer har i samarbejde med Datatilsynet i februar 2019 udarbejdet en ny type revisorerklæring, som skal give sikkerhed for, at databehandleren har orden i procedurer og regler for beskyttelse af persondata.

Revisorerklæringen har fået navnet "Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med [dataansvarlig]" og kan findes på FSR's hjemmeside.

Det fremgår af figur 7, at myndighederne har ført én eller flere former for tilsyn med deres databehandlere for 77 % af deres it-systemer. 6 ud af de 17 myndigheder har ført tilsyn for alle deres systemer. For 41 % af de udførte tilsyn gælder, at der udelukkende er indhentet en generel revisorerklæring. Det betyder, at uafhængige revisorer har ført tilsyn med databehandlerens generelle informationssikkerhed eller it-kontroller, men ikke har taget stilling til, om databehandleren overholder kravene i databehandleraftalen for det specifikke system.

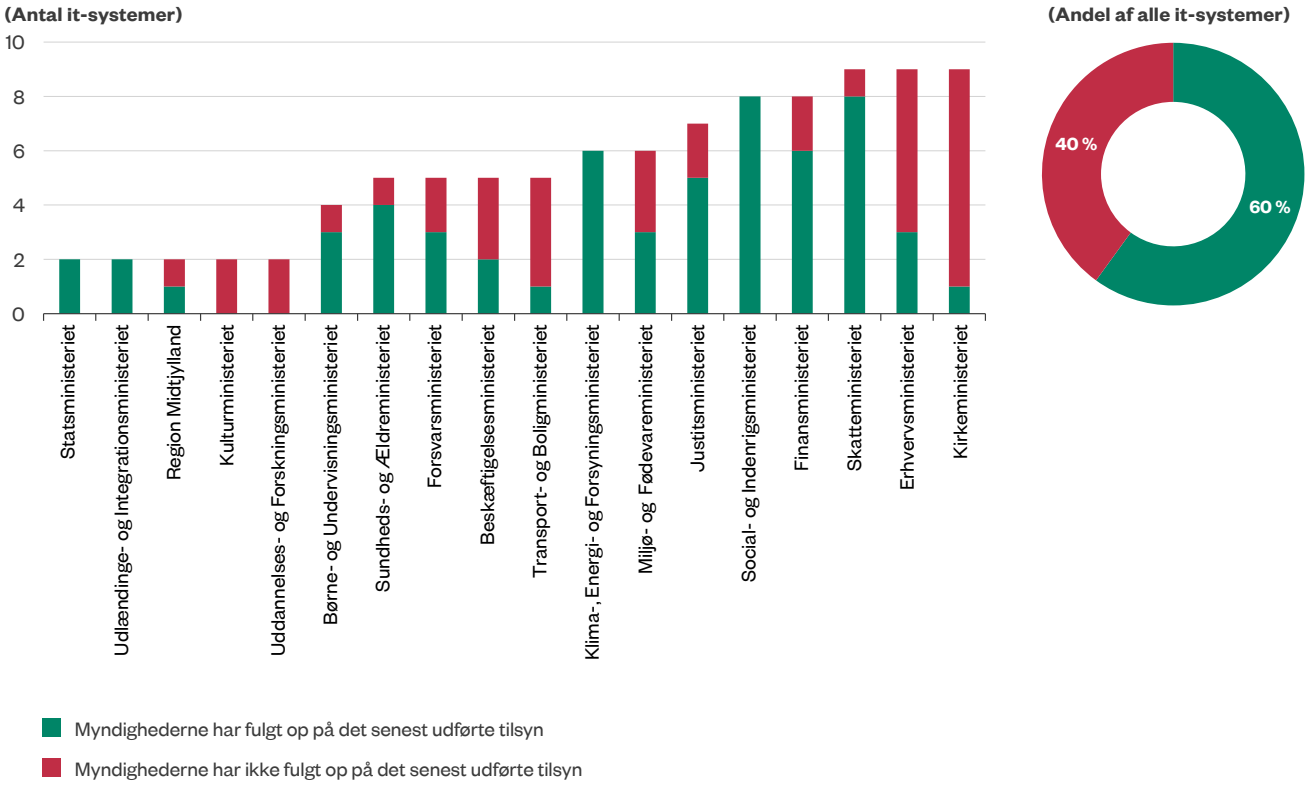
Myndighederne har ikke ført nogen form for tilsyn med deres databehandlere for 23 % af deres it-systemer. For alle disse gælder, at der er gået mindst 1 år, siden databehandleraftalen blev indgået. Udlændinge- og Integrationsministeriet, Kulturministeriet og Uddannelses- og Forskningsministeriet har ikke ført tilsyn for nogen af deres systemer.

Opfølgning på udførte tilsyn

52. Figur 8 viser, om myndighederne har fulgt op på deres senest udførte tilsyn. En opfølgning kan fx være, at myndigheden har sendt opfølgende spørgsmål til databehandleren, eller at myndigheden har konstateret i en intern mail, at tilsynet ikke gav anledning til yderligere handlinger over for databehandleren.

Figur 8

Opfølgning på udførte tilsyn pr. myndighed og samlet



Note: n=96 it-systemer fordelt på alle 18 myndigheder. Der indgår kun systemer, hvor der er ført tilsyn med databehandleren. Antallet af systemer i denne figur er højere end antallet i figur 7. Det skyldes, at der også indgår systemer, hvor databehandleraftalen er indgået for mindre end 1 år siden, eller hvor Statens It eller Statens Administration er databehandler, idet myndighederne også skal følge op på disse tilsyn. Der indgår ikke systemer, hvor der ikke er fulgt op på tilsyn, hvis det på undersøgelsestidspunktet var mindre end 3 måneder siden, at tilsynet blev udført. For hvert system indgår kun det senest udførte tilsyn.

Kilde: Rigsrevisionen.

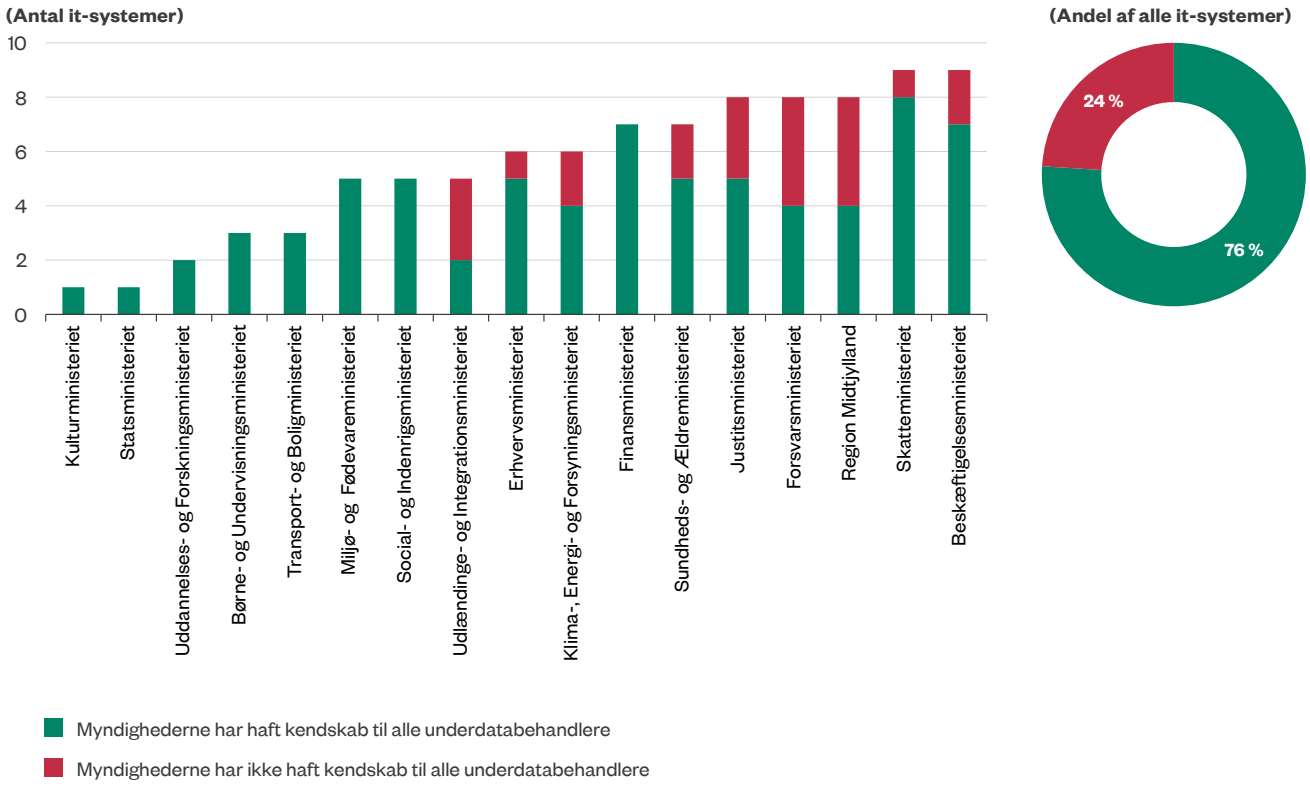
Det fremgår af figur 8, at myndighederne har fulgt op på 60 % af deres udførte tilsyn. Social- og Indenrigsministeriet, Klima-, Energi- og Forsyningsministeriet, Udlændinge- og Integrationsministeriet og Statsministeriet har fulgt op på alle deres udførte tilsyn. Myndighederne har omvendt for 40 % af it-systemerne ikke kunnet dokumentere, at de har fulgt op på de udførte tilsyn. For alle disse gælder, at det er mindst 3 måneder siden, at tilsynet blev udført. 6 ud af de 18 myndigheder har fulgt op på mindre end halvdelen af deres udførte tilsyn.

Kendskab til underdatabehandlere

53. Hvis myndigheden ikke fører tilsyn med sin databehandler, er der en risiko for, at myndigheden ikke har et opdateret og retvisende billede af, hvordan databehandlingen foregår, herunder hvilke underdatabehandlere der benyttes. Ifølge GDPR skal den dataansvarlige godkende brugen af underdatabehandlere og dermed have kendskab til, hvilke underdatabehandlere der behandler persondata. Figur 9 viser, om myndighederne har haft kendskab til alle underdatabehandlere for de it-systemer, hvor der benyttes underdatabehandlere.

Figur 9

Kendskab til alle underdatabehandlere pr. myndighed og samlet



Note: n=93 it-systemer fordelt på 17 myndigheder. Der indgår kun systemer i figuren, hvor der anvendes underdatabehandlere. For de resterende 55 systemer har databehandleren oplyst, at der ikke anvendes underdatabehandlere. Kirkeministeriet indgår ikke i opgørelsen, idet ministeriet ikke benytter underdatabehandlere for nogen af sine 9 systemer i undersøgelsen.

Kilde: Rigsrevisionen.

Det fremgår af figur 9, at myndighederne for 76 % af it-systemerne, hvor der benyttes underdatabehandlere, har haft kendskab til alle underdatabehandlere. 8 ud af de 17 myndigheder har haft kendskab til alle underdatabehandlere for alle deres systemer. For 24 % af systemerne har myndighederne imidlertid ikke haft kendskab til alle underdatabehandlere, som behandler deres persondata. Det betyder, at der er mindst én underdatabehandler, som har behandlet persondata uden myndighedens forudgående kendskab. Udlændinge- og Integrationsministeriet, Forsvarsministeriet og Region Midtjylland har kun haft kendskab til alle underdatabehandlere for halvdelen eller færre af deres systemer, hvor underdatabehandlere behandler deres persondata.

54. Som følge af vores undersøgelse er myndighederne blevet opmærksomme på en række tilfælde, hvor databehandlerne har gjort brug af underdatabehandlere, som myndighederne ikke havde kendskab til. Boks 4 giver 3 eksempler på tilfælde, hvor myndighederne ikke var klar over, at deres databehandler gjorde brug af underdatabehandlere.

Boks 4

Eksempler på myndigheder, der ikke havde kendskab til alle underdatabehandlere

Forsvarsministeriets Materiel- og Indkøbsstyrelse
Forsvarsministeriets Materiel- og Indkøbsstyrelse (FMI) har anvendt en privat it-leverandør til at opbevare følsomme og fortrolige personoplysninger. FMI fandt i forbindelse med undersøgelsen ud af, at leverandøren havde benyttet en global cloud-udbyder som underdatabehandler, uden at FMI havde godkendt eller var blevet orienteret herom. FMI har efterfølgende opsagt samarbejdet med leverandøren.

Arbejdstilsynet
Arbejdstilsynet har anvendt en privat it-leverandør til behandling af personoplysninger, som omfatter følsomme personoplysninger og cpr-numre. Arbejdstilsynet fandt i forbindelse med undersøgelsen ud af, at databehandleren opbevarede data i Norge og anvendte en global cloud-udbyder som underdatabehandler, uden at Arbejdstilsynet var bekendt hermed. Arbejdstilsynet var derimod af den opfattelse, at data blev opbevaret i Danmark, og at databehandleren ikke anvendte underdatabehandlere. Der var ikke i databehandleraftalen taget stilling til, om Arbejdstilsynet skulle godkende underdatabehandlere. Arbejdstilsynet har afsluttet samarbejdet med den pågældende databehandler.

Sundhedsdatastyrelsen
Sundhedsdatastyrelsen har anvendt en privat it-leverandør til at opbevare Landspatientregisteret. Sundhedsdatastyrelsen fandt i forbindelse med undersøgelsen ud af, at databehandleren uden styrelsens godkendelse anvender en underdatabehandler, selv om det fremgår af databehandleraftalen, at Sundhedsdatastyrelsen specifikt skal godkende brugen af underdatabehandlere.

Godkendelse af underdatabehandlere
Ifølge GDPR skal den dataansvarlige enten give en generel eller en specifik godkendelse af alle underdatabehandlere og dermed have kendskab til de underdatabehandlere, der behandler den dataansvarliges persondata.

Generel godkendelse betyder, at databehandleren kan anvende nye underdatabehandlere uden en forudgående specifik godkendelse fra den dataansvarlige myndighed. Myndigheden skal dog underrettes om nye underdatabehandlere og kan eventuelt gøre indsigelser.

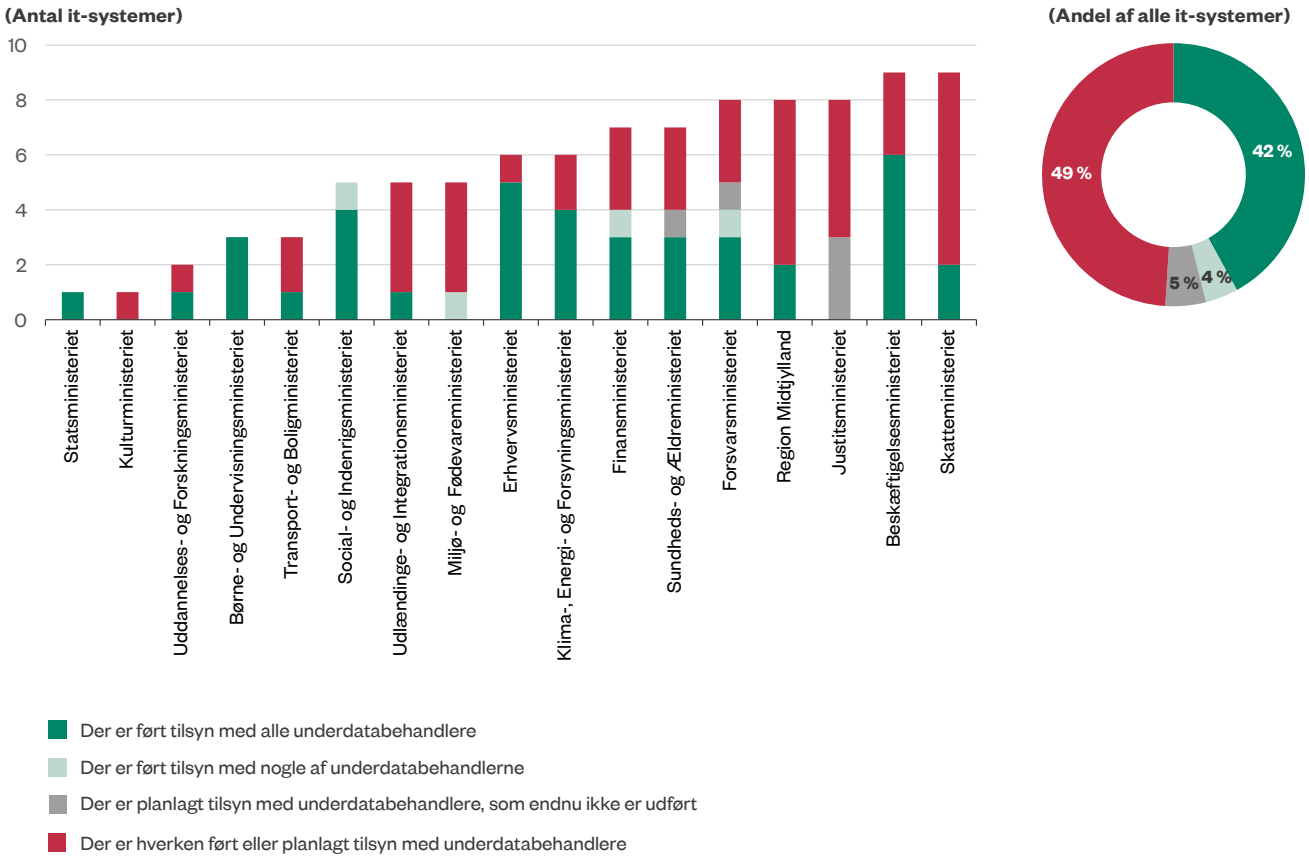
Specifik godkendelse betyder, at databehandleren ikke må benytte en ny underdatabehandler, før myndigheden specifikt har godkendt den nye underdatabehandler.

Tilsyn med underdatabehandlere

55. Det er Datatilsynets vurdering, at den dataansvarlige skal leve op til kravet om ansvarlighed og kunne påvise, om databehandlingen hos underdatabehandlere overholder databehandleraftalen og reglerne i GDPR. Vi har derfor undersøgt, om myndighederne har sikret, at der er ført tilsyn med underdatabehandlere, dvs. at enten myndigheden selv eller databehandleren har ført tilsyn med underdatabehandlere. Figur 10 viser, om myndighederne har sikret, at der er ført tilsyn med underdatabehandlere af myndighedernes it-systemer.

Figur 10

Tilsyn med underdatabehandlere



Note: n=93 it-systemer fordelt på 17 myndigheder. Der indgår kun systemer, hvor der anvendes underdatabehandlere. For de resterende 55 systemer har databehandleren oplyst, at der ikke anvendes underdatabehandlere. Kirkeministeriet indgår ikke i opgørelsen, idet ministeriet ikke benytter underdatabehandlere for nogen af sine 9 systemer i undersøgelsen.

Kilde: Rigsrevisionen.

Det fremgår af figur 10, at myndighederne ikke har sikret, at der er ført eller planlagt tilsyn med underdatabehandlerne for 49 % af deres it-systemer, hvor der benyttes underdatabehandlere. 7 ud af de 17 myndigheder har for over halvdelen af deres systemer ikke sikret, at der er ført eller planlagt tilsyn med deres underdatabehandlere. Myndighederne har dog sikret, at der er ført tilsyn med alle underdatabehandlere for 42 % af systemerne. 6 ud af de 17 myndigheder har sikret, at der er ført tilsyn med alle underdatabehandlere for mindst to tredjedele af deres systemer, hvor der benyttes underdatabehandlere.

Resultater

Undersøgelsen viser, at myndighederne for 24 % af it-systemerne med følsomme eller fortrolige persondata ikke har en plan for at føre tilsyn med deres databehandlere. Desuden findes der for 23 % af systemerne kun en overordnet tilsynsplan, som ikke forholder sig til de specifikke systemer. Det betyder, at myndighederne for knap halvdelen af systemerne ikke har taget stilling til, hvor ofte eller hvordan der skal føres tilsyn med databehandlerne for de specifikke systemer, som opbevarer følsomme eller fortrolige persondata.

Undersøgelsen viser desuden, at myndighederne for 23 % af systemerne ikke har ført tilsyn med deres databehandlere. Undersøgelsen viser også, at myndighederne ikke har kunnet dokumentere, at der er blevet fulgt op på 40 % af deres udførte tilsyn. Det betyder efter Rigsrevisionens vurdering, at disse tilsyn ikke har tjent deres egentlige formål, når myndigheden ikke forholder sig til resultaterne af tilsynet.

Hvis myndighederne ikke fører tilsyn med deres databehandlere, er der bl.a. risiko for, at de ikke har et opdateret og retvisende billede af, hvilke underdatabehandlere der behandler deres persondata. Undersøgelsen viser, at myndighederne ikke har haft kendskab til alle underdatabehandlere for 24 % af de systemer, hvor underdatabehandlere behandler følsomme eller fortrolige persondata. Udlændinge- og Integrationsministeriet, Forsvarsministeriet og Region Midtjylland har kun haft kendskab til alle underdatabehandlere for halvdelen eller færre af deres systemer, hvor underdatabehandlere behandler deres persondata.

Endelig viser undersøgelsen, at myndighederne for 49 % af systemerne ikke har sikret, at der er ført tilsyn med underdatabehandlere, som behandler følsomme eller fortrolige persondata. Det betyder, at myndighederne i disse tilfælde ikke har haft vished om, hvorvidt underdatabehandlerne overholder databehandleraftalen og databeskyttelsesreglerne.

3. Understøttelse af myndighedernes styring af databehandlere

Delkonklusion

Justitsministeriet, herunder Datatilsynet, og Finansministeriet har ikke i tilstrækkelig grad understøttet de øvrige myndigheders styring af databehandlere.

Justitsministeriet, Datatilsynet og Digitaliseringsstyrelsen har udgivet 20 vejledninger, som de vurderede var nødvendige for at understøtte myndighederne i deres implementering af GDPR. Det finder Rigsrevisionen positivt.

8 af de 20 vejledninger udkom imidlertid, efter GDPR blev gældende. Rigsrevisionen finder det uhensigtsmæssigt, at vejledningerne er kommet så sent, da offentlige myndigheder og private virksomheder dermed har manglet flere relevante vejledninger på det tidspunkt, hvor GDPR blev gældende. Datatilsynets vejledning om risikovurderinger og Digitaliseringsstyrelens vejledning om cloud-services udkom mere end 1 år efter GDPR.

Rigsrevisionen finder det utilfredsstillende, at Justitsministeriet endnu ikke har udgivet hverken en bekendtgørelse eller en vejledning om lokationskravet (tidligere krigsreglen), som bestemmer, hvilke systemer der af hensyn til statens sikkerhed skal opbevares i Danmark. Særligt den manglende vejledning har skabt usikkerhed blandt myndighederne om, hvilke systemer der potentielt skal opbevares i Danmark.

Rigsrevisionens spørgeskemaundersøgelse viser, at størstedelen af myndighederne vurderer, at det samlede vejledningsmateriale har understøttet dem i at udarbejde databehandleraftaler. Myndighederne vurderer dog også, at vejledningsmaterialet i mindre grad har understøttet deres arbejde med at udarbejde risikovurderinger og føre tilsyn med deres databehandlere.

Datatilsynet har ikke ført et risikobaseret tilsyn. Datatilsynet har ikke udarbejdet risikoanalyser til at understøtte planlægningen af sit tilsyn og har ikke opdateret sin strategi, siden GDPR blev gældende i maj 2018. Datatilsynet har ikke kunnet dokumentere, at de tilsyn, som Datatilsynet har planlagt, er udvalgt ud fra en risikobetragtning. Det betyder, at det er usikkert, om Datatilsynet har anvendt de tilgængelige resurser til at føre tilsyn, der hvor risikoen er størst.

Datatilsynet har kun afsluttet 8 tilsyn med offentlige myndigheder og 14 tilsyn med private virksomheder, siden GDPR blev gældende. Det betyder, at der er få afgørelser, som myndighederne kan benytte som fortolkningsbidrag til at overholde GDPR. Det betyder også, at risikoen for at blive opdaget i overtrædelser af GDPR - og dermed tilsynenes præventive effekt - har været relativt lav. Ingen af de afsluttede planlagte tilsyn blev afsluttet inden for 6 måneder, selv om Datatilsynet har et mål om, at 80 % af tilsynene skal være afsluttet inden for 6 måneder. Hvis Datatilsynet havde afsluttet 80 % af sine planlagte tilsyn inden for 6 måneder, kunne Datatilsynet have afsluttet mindst 50 tilsyn inden udgangen af 2019.

56. Dette kapitel handler om, hvorvidt Justitsministeriet, herunder Datatilsynet, og Finansministeriet i tilstrækkelig grad har understøttet de øvrige myndigheders styring af databehandlere. Vi undersøger de 3 myndigheders vejledningsindsats, og om Datatilsynet har ført et risikobaseret tilsyn.

3.1. Vejledningsindsats

57. Vi har undersøgt, om Justitsministeriet, herunder Datatilsynet, og Digitaliseringsstyrelsen under Finansministeriet rettidigt har vejledt de øvrige myndigheder i forbindelse med GDPR. Vi har desuden undersøgt, om vejledningerne har understøttet myndighederne i deres arbejde med styring af databehandlere.

58. Det er Datatilsynets vurdering, at den øgede bevidsthed hos offentlige og private aktører har nødvendiggjort yderligere og mere fyldestgørende vejledning om udvalgte emner i forhold til databeskyttelsesreglerne. Det var også Justitsministeriets vurdering, at der var et stort behov for, at der i løbet af 2017 blev udarbejdet vejledninger om centrale emner i GDPR.

59. Justitsministeriet har oplyst, at ministeriets forpligtelse til at vejlede offentlige myndigheder om databeskyttelsesreglerne ikke går længere end kravet om god forvaltningsskik. Det følger af kravet om god forvaltningsskik, at en myndighed i et vist omfang skal sørge for fornøden information om sit ressortområde.

Rettidig vejledning i forbindelse med GDPR

60. I april 2016 igangsatte Justitsministeriet et projektarbejde, der havde til formål at indrette dansk lovgivning efter GDPR og udbrede kendskabet til de nye regler. En styregruppe bestående af Justitsministeriet, Datatilsynet, Digitaliseringsstyrelsen og Erhvervsstyrelsen var ansvarlig for projektarbejdets gennemførelse. Styregruppen skulle bl.a. hurtigt afklare de nye krav i GDPR og på den måde danne grundlag for at udarbejde praktisk anvendelige vejledninger. Projektarbejdet mundede bl.a. ud i en omfangsrig betænkning, som beskriver, hvordan GDPR påvirker øvrig dansk lovgivning.

Styregruppen fordelte rollen som ansvarlig for 12 vejledninger mellem Justitsministeriet, Datatilsynet og Digitaliseringsstyrelsen. Det var planen, at den sidste af de 12 vejledninger skulle udkomme i januar 2018 – altså 4 måneder før, GDPR blev gældende. Ud over de 12 vejledninger, som blev aftalt i styregruppen, udgav Datatilsynet og Justitsministeriet yderligere 8 vejledninger relateret til GDPR og databeskyttelse. Samlet set har Datatilsynet udgivet størstedelen af vejledningerne. Datatilsynet har oplyst, at behovet for at udarbejde de vejledninger, som ikke var en del af projektarbejdet, først opstod, efter GDPR blev gældende. Det er Datatilsynets opfattelse, at de 8 vejledninger derfor ikke skulle udarbejdes, inden GDPR blev gældende.

61. Figur 11 viser, hvornår de 12 planlagte vejledninger udkom i forhold til GDPR (25. maj 2018) og i forhold til den sidste planlagte vejledning i projektarbejdets udgivelsesplan (januar 2018), samt hvornår de 8 yderligere vejledninger udkom i forhold til GDPR.

Figur 11

Oversigt over, hvornår de 20 vejledninger udkom

Note: Figuren er baseret på første udgivelse af vejledningerne. Nogle vejledninger er sidenhen blevet opdateret.

Kilde: Rigsrevisionens opgørelse på baggrund af offentliggjorte vejledninger og tidsplaner.

Det fremgår af figur 11, at 7 af de 12 planlagte vejledninger udkom mindst 4 måneder før GDPR, som de skulle ifølge projektarbejdets udgivelsesplan. 2 af de planlagte vejledninger udkom inden for de sidste 4 måneder op til GDPR, mens de resterende 3 planlagte vejledninger udkom, efter GDPR blev gældende. Digitaliseringsstyrelsens vejledning om cloud computing udkom først i november 2019, ca. 1½ år efter GDPR. Digitaliseringsstyrelsen igangsatte arbejdet i oktober 2017. I december 2017 og igen i februar 2018 tilkendegav Datatilsynet, at det var vanskeligt at se, at vejledningen i sin nuværende form var egnet som en vejledning om fortolkning af GDPR. Digitaliseringsstyrelsen har oplyst, at styrelsen efterfølgende afventede en opdateret vejledning fra Datatilsynet om overførsel af personoplysninger til tredjelande, som udkom i juni 2019, og Justitsministeriets vejledning om lokationskravet (tidligere krigsreglen), der endnu ikke er udkommet.

Forsinkelsen af cloud-vejledningen har betydet, at myndighederne i nogle tilfælde har været usikre på, hvordan cloud-services kan anvendes inden for databeskyttelsesreglerne. 14 % af myndighederne har i vores spørgeskemaundersøgelse givet udtryk for, at de havde spørgsmål vedrørende cloud, som de ikke kunne få svar på gennem den eksisterende vejledningsindsats.

Det fremgår også af figuren, at 5 af de 8 ikke-planlagte vejledninger udkom efter GDPR, mens de resterende 3 udkom, inden GDPR blev gældende. Af de 5 vejledninger var det særligt vejledningen om risikovurderinger, som udkom lang tid efter, at GDPR blev gældende. Datatilsynet har oplyst, at behovet for en vejledning om risikovurderinger først opstod i forbindelse med, at Rådet for Digital Sikkerhed kontaktede Datatilsynet i begyndelsen af 2019. Datatilsynet har også oplyst, at reglerne om risikovurderinger var gældende under persondataloven, og at myndighederne i styregruppen prioriterede at udgive vejledninger om nye regler. Endelig har Datatilsynet oplyst, at forholdene vedrørende risikovurderinger beskrives i Justitsministeriets betænkning. Det er imidlertid Rigsrevisionens vurdering, at betænkningen i sig selv ikke kan stå i stedet for en praktisk anvendelig vejledning, og at risikovurderingen er et helt grundlæggende element i implementeringen af GDPR, som Datatilsynet af egen drift burde have vejledt om tidligere.

62. Justitsministeriet vurderer, at ministeriets vejledningsindsats er gået langt videre, end hvad ministeriet har været forpligtet til ifølge kravet om god forvaltningsskik. Rigsrevisionen er enig i, at Justitsministeriet ikke er yderligere forpligtet til at vejlede om databeskyttelsesreglerne, end hvad der følger af kravet om god forvaltningsskik. Rigsrevisionen konstaterer imidlertid, at Justitsministeriet selv har fundet det relevant at vejlede om databeskyttelsesreglerne, og finder det derfor vigtigt – ud fra hensynet til en rettidig implementering af GDPR – at de relevante vejledninger blev udgivet, inden GDPR blev gældende.

63. Flere myndigheder oplyser i forbindelse med vores spørgeskemaundersøgelse, at det har været en udfordring, at en række vejledninger udkom meget sent i forhold til GDPR. Desuden viser spørgeskemaundersøgelsen, at 30 % af de adspurgte myndigheder vurderer, at de selv har igangsat initiativer, som kunne have været undgået, hvis vejledningerne havde været mere konkrete, mere omfangsrige eller var udkommet tidligere. Datatilsynet har i den forbindelse oplyst, at Datatilsynet kun kan udøve vejledning af mere generel karakter. Det skyldes, at konkret rådgivning kan fratage Datatilsynet muligheden for efterfølgende at føre tilsyn med overholdelsen af reglerne.

Datatilsynet vurderer derfor, at der kan være tilfælde, hvor det vil være nødvendigt for den enkelte myndighed at inddrage ekstern bistand. Rigsrevisionen er enig i, at Datatilsynets rådgivning kan blive så konkret, at det kan være vanskeligt efterfølgende at føre tilsyn med overholdelsen af reglerne. Rigsrevisionen kan ikke vurdere, om vejledningerne har været tilstrækkeligt omfangsrige eller konkrete, men vurderer udelukkende, om de er udkommet rettidigt. Boks 5 beskriver 2 eksempler på initiativer, som myndigheder tog, og som myndighederne selv vurderede kunne have været undgået, hvis vejledningerne var udkommet tidligere.

Boks 5

Eksempler på initiativer, som myndighederne vurderede kunne have været undgået, hvis vejledningerne var udkommet tidligere

Klima-, Energi- og Forsyningsministeriet
Klima-, Energi- og Forsyningsministeriets databeskyttelsesrådgiver tog initiativ til, at der blev indhentet bistand fra et revisionshus til at udvikle en metodik for at gennemføre risikovurderinger, idet Datatilsynets vejledning om risikovurderinger først udkom 1 år efter, at GDPR blev gældende.

Region Midtjylland
Region Midtjylland har i samarbejde med de øvrige regioner udarbejdet egne skabeloner til bl.a. databehandleraftaler og konsekvensanalyser, fordi regionen har oplevet, at vejledningerne generelt er udkommet sent og har været for overordnede i deres indhold til at være retningsgivende i arbejdet med outsourcing af persondata. Herunder har regionen oplevet, at vejledningen om dataansvarlige og databehandlere ikke skaber klarhed om, hvornår der er tale om behandling af personoplysninger, som kræver en databehandleraftale. Forsinkelsen af vejledningen om brug af cloud og vejledningen om lokationskravet (tidligere krigsreglen) har desuden været medvirkende til, at regionen har været tilbageholdende med at anvende cloud-løsninger.

Spørgeskemaundersøgelsen viser også, at næsten 75 % af de adspurgte myndigheder i høj eller meget høj grad vurderer, at vejledningsmaterialet har understøttet dem i at udarbejde databehandleraftaler, mens tallet kun var knap 30 %, hvad angår risikovurderinger og tilsyn. Det kan fx skyldes, at vejledningen om risikovurderinger først udkom mere end 1 år efter, at GDPR blev gældende.

Lokationskravet (tidligere krigsreglen)

64. Databeskyttelsesloven, som supplerer GDPR i dansk lovgivning, indeholder en særlig bestemmelse for nye eller genudbudte it-systemer, der har betydning for statens sikkerhed – det såkaldte lokationskrav (tidligere krigsreglen). Lokationskravet bestemmer, at disse systemer skal opbevares på servere i Danmark. Der kan være tale om systemer med oplysninger, som fremmede magter kunne have interesse i, eller hvor tabt adgang er en trussel mod, at offentlige myndigheder kan udfylde deres funktion. Ofte vil der også være tale om systemer, som indeholder store mængder af personoplysninger.

Af lovforslaget til databeskyttelsesloven fra oktober 2017 fremgik det, at justitsministeren skulle udstede en bekendtgørelse, der gav et overblik over, hvilke it-systemer der er omfattet af lokationskravet. Det fremgik også af lovforslaget, at justitsministeren kunne udarbejde nærmere retningslinjer, som skulle følges, når myndigheder skal vurdere, om deres it-systemer kan være omfattet af lokationskravet. Justitsministeriet planlagde at udfolde de nærmere retningslinjer i form af en vejledning om lokationskravet. Vejledningen skulle give myndighederne viden om, hvornår et system *kan* være omfattet af lokationskravet og derfor skal indmeldes til Justitsministeriet, som i sidste ende vurderer, om systemet er omfattet af lokationskravet.

Pr. 4. maj 2020 er hverken bekendtgørelse eller vejledning om lokationskravet offentliggjort.

65. Justitsministeriet sendte udkast til bekendtgørelse og vejledning i høring i juli 2019. Flere myndigheder gav i deres høringssvar udtryk for, at der var en række uklarheder i vejledningen, herunder:

- uklarhed om, hvornår it-systemer kan være omfattet af lokationskravet, fx at det er uklart, hvilke kriterier der lægges vægt på i vurderingen af, om et system kan være omfattet af lokationskravet
- uklarhed om, hvad lokationskravet omfatter, fx om lokationskravet gælder al behandling af data eller kun opbevaring af data
- uklarhed om, i hvilken udstrækning it-systemer, der er omfattet af lokationskravet, stadig er omfattet af reglerne i GDPR.

Justitsministeriet lægger vægt på, at det er de enkelte ministerier, som skal henvende sig til Justitsministeriet, hvis der er tvivl om, hvorvidt et it-system kan være omfattet af lokationskravet – uanset om der findes en vejledning herom eller ej. Ikke desto mindre er formålet med Justitsministeriets vejledning netop at understøtte myndighederne i at vurdere, om deres systemer *kan* være omfattet af lokationskravet, og dermed om de i første omgang skal rette henvendelse til Justitsministeriet.

Resultater

Undersøgelsen viser, at Justitsministeriet, herunder Datatilsynet, og Digitaliseringsstyrelsen har udgivet 20 vejledninger i forbindelse med GDPR. Det finder Rigsrevisionen positivt, da vejledningerne har kunnet understøtte en styrket overholdelse af databeskyttelsesreglerne blandt offentlige myndigheder. Rigsrevisionen finder det imidlertid uhensigtsmæssigt, at en række vejledninger udkom kort tid før GDPR, og at 8 vejledninger først udkom, efter GDPR blev gældende. Væsentlige vejledninger om risikovurderinger og cloud-services udkom således mere end 1 år efter GDPR. 14 % af myndighederne har i forbindelse med Rigsrevisionens spørgeskemaundersøgelse angivet, at de har manglet vejledningsmateriale om cloud-services. 30 % af myndighederne vurderede, at de i nogle tilfælde selv har igangsat initiativer på baggrund af GDPR, som efter deres vurdering kunne have været undgået, hvis vejledningerne havde været mere konkrete, mere omfangsrige eller var udkommet tidligere.

Undersøgelsen viser også, at størstedelen af myndighederne vurderer, at vejledningsmaterialet har understøttet deres arbejde med at udarbejde databehandleraftaler, men at vejledningsmaterialet i mindre grad har understøttet deres arbejde med at udarbejde risikovurderinger og føre tilsyn med databehandlere. Det kan bl.a. skyldes, at vejledningen om risikovurderinger først udkom mere end 1 år efter, at GDPR blev gældende.

Endelig viser undersøgelsen, at Justitsministeriet knap 2 år efter, at databeskyttelsesloven er trådt i kraft, endnu ikke har offentliggjort en bekendtgørelse om lokationskravet, som ministeriet skal ifølge lovforslaget til databeskyttelsesloven fra oktober 2017. Justitsministeriet har heller ikke udgivet den planlagte vejledning om lokationskravet. Det har betydet, at retningslinjerne for, hvilke systemer myndighederne skal indmelde til Justitsministeriet, ikke har været klare, og at flere myndigheder derfor har været i tvivl om, hvilke systemer der af hensyn til statens sikkerhed kan være omfattet af lokationskravet og dermed skal opbevares i Danmark.

3.2. Datatilsynets tilsyn

66. Vi har undersøgt, om Datatilsynet har ført et risikobaseret tilsyn. Datatilsynets tilsynsaktivitet er vigtig, fordi Datatilsynets offentliggjorte tilsynsafgørelser er blandt de centrale fortolkningsbidrag til myndigheders forståelse af databeskyttelsesreglerne. Desuden giver tilsynene viden om, hvorvidt reglerne overholdes i praksis, ligesom tilsynene kan have en præventiv effekt, fordi myndigheder, der ikke overholder databeskyttelsesreglerne, kan få dårlig omtale og betragtelige bøder. Datatilsynets opgaver er nærmere beskrevet i boks 6.

Boks 6

Datatilsynets opgaver

Datatilsynet vejleder og fører tilsyn med det offentlige og private virksomheder. Datatilsynets opgaver er beskrevet i GDPR's artikel 57. Af artiklen fremgår 22 nærmere specificerede opgaver. Her fremgår det bl.a. om Datatilsynets rådgivnings- og vejledningsindsats, at Datatilsynet skal fremme offentlighedens, Folketingets, regeringens, dataansvarliges, databehandleres og borgeres kendskab til reglerne i GDPR.

Desuden bidrager Datatilsynet til det fælleseuropæiske arbejde med at udarbejde retningslinjer og vejledninger samt yder telefonisk vejledning, deltager på konferencer m.m.

I 2019 var Datatilsynet bevilget 63 årsværk sammenlignet med 34 årsværk i 2017. Datatilsynet er i 2019 ikke kommet i mål med de nødvendige ansættelser og har derfor kun været 56 årsværk. I perioden, fra GDPR blev gældende den 25. maj 2018 til 1. januar 2020, har Datatilsynet modtaget 9.978 anmeldelser om brud på persondatasikkerheden. Samlet set har Datatilsynet oplevet en stigning på ca. 400 % i antallet af nyoprettede sager fra 2017 til 2019.

Datatilsynets planlægning af tilsyn

67. Datatilsynet har ikke gennemført analyser af, hvilke behandlinger af persondata der er forbundet med en særlig risiko i forhold til reglerne i GDPR. Datatilsynet har heller ikke udarbejdet en ny overordnet strategi, efter GDPR blev gældende, og har derfor fortsat planlagt sit tilsyn på baggrund af strategien for 2016-2018, som blev udarbejdet i 2015.

Datatilsynet er i gang med at gennemføre en evaluering af sin tilsynsvirksomhed, som skal indgå i et samlet projekt om en ny overordnet strategi for Datatilsynet.

68. Det fremgår af Datatilsynets strategi for 2016-2018, at Datatilsynet i sine tilsynsplaner vil have fokus på behandlinger af personoplysninger, som indebærer en særlig risiko for de registreredes rettigheder. Dette kan ifølge Datatilsynet omfatte temaer som sletning af personoplysninger, anmeldelser om brud på persondatasikkerheden, registreredes ret til indsigt i, hvilke oplysninger der er registreret om dem og behandling af personoplysninger hos databehandlere. Datatilsynet har oplyst, at Datatilsynet har valgt at føre tilsyn med aktører, som behandler følsomme personoplysninger eller en stor mængde personoplysninger. Datatilsynet har ikke kunnet dokumentere, at den faktiske planlægning af tilsyn er baseret på disse overvejelser.

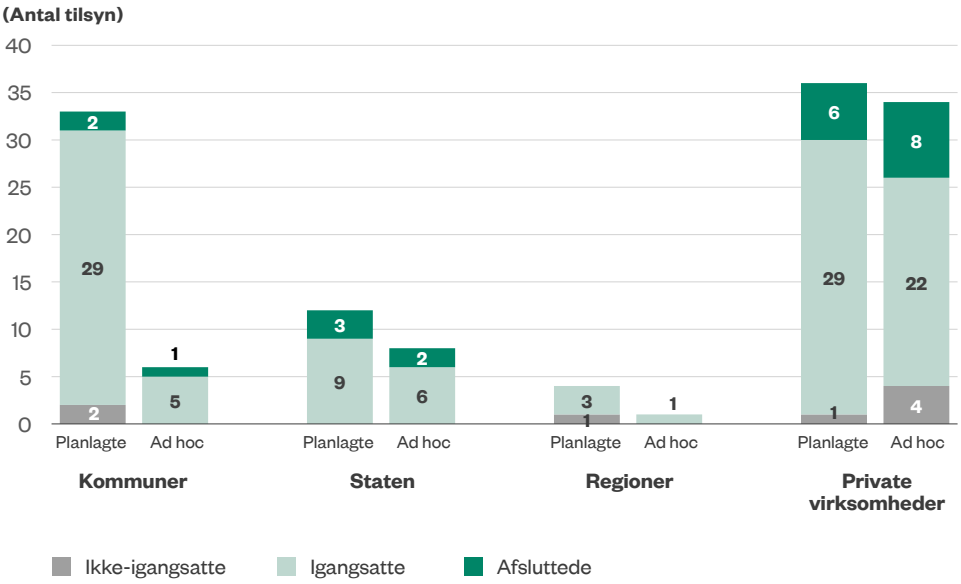
69. Datatilsynet har, siden GDPR blev gældende, udarbejdet halvårlige tilsynsplaner. Tilsynsplanerne indeholder 85 planlagte tilsyn for perioden 25. maj 2018 til udgangen af 2019. De planlagte tilsyn dækker over 36 tilsyn med private virksomheder, 33 tilsyn med kommuner, 4 tilsyn med regioner og 12 tilsyn med statslige myndigheder.

Datatilsynets gennemførte tilsyn

70. Figur 12 viser Datatilsynets planlagte tilsyn og ad hoc-tilsyn, fra GDPR blev gældende til 1. januar 2020.

Figur 12

Datatilsynets planlagte tilsyn og ad hoc-tilsyn efter GDPR fordelt på kommuner, staten, regioner og private virksomheder



Note: Figuren viser, hvor mange af de 85 planlagte tilsyn og 49 ad hoc-tilsyn som Datatilsynet har igangsat eller afsluttet siden GDPR. De tilsyn, som hverken er igangsat eller afsluttet, fremgår som ikke-igangsatte. Vi forstår et tilsyn som *afsluttet*, når Datatilsynet har offentliggjort en udtalelse på sin hjemmeside. Vi forstår et tilsyn som *igangsat*, når Datatilsynet har sendt et åbningsbrev, gennemført et tilsynsbesøg eller indhentet materiale, men endnu ikke har offentliggjort en udtalelse på sin hjemmeside. Figuren indeholder også tilsyn med retshåndhævende myndigheder, som er underlagt retshåndhævelsesloven.

Kilde: Rigsrevisionen på baggrund af data fra Datatilsynet og Datatilsynets hjemmeside.

Det fremgå af figur 12, at Datatilsynet har afsluttet 11 ud sine 85 planlagte tilsyn, mens Datatilsynet har igangsat yderligere 70 af sine planlagte tilsyn. 4 af de planlagte tilsyn er endnu ikke igangsat. Desuden fremgår det det, at Datatilsynet har afsluttet 11 ad hoc-tilsyn, igangsat 34 ad hoc-tilsyn og planlagt 4 ad hoc-tilsyn, som endnu ikke er igangsat. Samlet set har Datatilsynet – ca. 1½ år efter GDPR – afsluttet 22 tilsyn, hvoraf de 8 vedrører offentlige myndigheder.

71. Datatilsynet har et mål om, at 80 % af Datatilsynets tilsyn skal afsluttes senest 6 måneder efter, at de er igangsat. De 11 afsluttede planlagte tilsyn tog i gennemsnit 9 måneder at afslutte, og ingen af tilsynene overholdt Datatilsynets egen målsætning om at afslutte tilsyn inden for 6 måneder. 45 af de 70 igangsatte planlagte tilsyn har været i gang i mere end 6 måneder, herunder 9 tilsyn i mere end 1 år. Datatilsynet har oplyst, at muligheden for at pålægge større bøder, efter GDPR blev gældende, har haft en negativ betydning for Datatilsynets sagsbehandlingstider for tilsynssager. Det skyldes dels, at der er særligt høje krav til bevissikkerhed i straffesager, dels at dem, der er underlagt tilsyn, i højere grad end tidligere udfordrer Datatilsynet i forbindelse med tilsyn og stiller flere spørgsmål til processen.

Planlagte tilsyn
Planlagte tilsyn er tilsyn, som iværksættes på baggrund af Datatilsynets halvårlige tilsynsplaner.

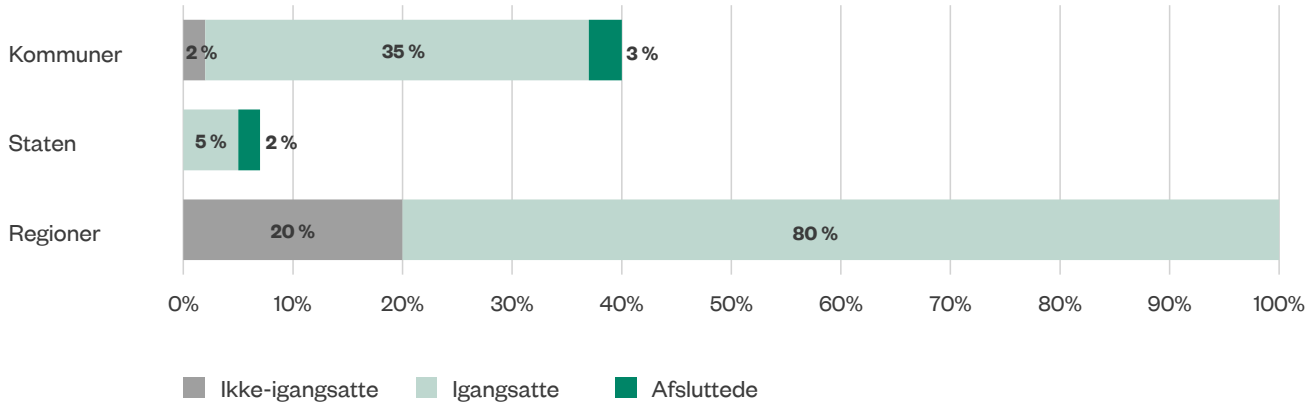
Ad hoc-tilsyn
Ad hoc-tilsyn er tilsyn, som iværksættes som følge af konkrete hændelser, fx medieomtale, klager og anmeldelser.

Datatilsynet skulle ifølge sin egen tilsynsplan have igangsat 64 af de planlagte tilsyn inden sommeren 2019. Hvis Datatilsynet havde opfyldt sit eget mål om at afslutte 80 % af tilsynene inden for 6 måneder, kunne Datatilsynet have afsluttet mindst 50 af de 64 planlagte tilsyn inden udgangen af 2019.

72. Figur 13 viser, hvor stor en andel af offentlige myndigheder der har været omfattet af Datatilsynets tilsyn (både planlagte og ad hoc), fra GDPR blev gældende til den 1. januar 2020.

Figur 13

Datatilsynets tilsyn (både planlagte og ad hoc) efter GDPR i forhold til det samlede antal offentlige myndigheder



Note: Opgørelsen er baseret på, at der i perioden har været 98 kommuner, 5 regioner og 318 statslige myndigheder. Kommuner og regioner er opgjort som samlede enheder, men vil hver især dække over forskellige forvaltninger, institutioner, sygehuse o.l. Antallet af statslige myndigheder er udledt på baggrund af Digitaliseringsstyrelsens åbne data om offentlige forvaltningsopgaver på form-online.dk. Udgangspunktet er, at der er tale om statslige myndigheder, som fremgår af finansloven. Opgørelsen af statslige myndigheder adskiller sig fra den opgørelse, som Digitaliseringsstyrelsen anvender i forbindelse med sin opfølgning på ISO 27001, som omfatter 105 statslige myndigheder. Digitaliseringsstyrelsens opgørelse omfatter imidlertid ikke statslige myndigheder som fx retsinstanser, ambassader og Nationalt Genom Center. Vi anvender derfor en bredere opgørelse af statslige myndigheder. Det betyder også, at opgørelsen omfatter mindre råd og nævn.

Kilde: Rigsrevisionen på baggrund af data fra Datatilsynet og Datatilsynets hjemmeside.

Det fremgår af figur 13, at Datatilsynets samlede tilsyn (både planlagte og ad hoc) omfatter 40 % af kommunerne, 7 % af staten og 100 % af regionerne. Dog dækker de afsluttede tilsyn kun 3 % af kommunerne, 2 % af staten og 0 % af regionerne. Opgjort på ministerområder omfatter de 5 afsluttede tilsyn inden for staten 3 ud af 18 ministerområder. Samlet set omfatter de planlagte tilsyn 10 ud af 18 ministerområder.

73. Ud over de omtalte tilsyn har Datatilsynet gennemført 128 tilsyn med statslige myndigheders, kommuners, regioners og private virksomheders udpegning af en databeskyttelsesrådgiver. Tilsynene blev udarbejdet på et skriftligt grundlag og indebar ikke fysiske besøg. De 128 tilsyn er beskrevet i boks 7.

Boks 7

Tilsyn med udpegning af en databeskyttelsesrådgiver

122 af de 128 tilsyn blev ført med offentlige myndigheder. Tilsynene afdækkede:

- om der var udpeget en databeskyttelsesrådgiver
- om databeskyttelsesrådgiverens kontaktoplysninger var sendt til Datatilsynet.

Tilsynene viste, at alle de offentlige myndigheder havde udpeget en databeskyttelsesrådgiver. 27 % af myndighederne havde imidlertid ikke sendt kontaktoplysninger til Datatilsynet.

Resultater

Undersøgelsen viser, at Datatilsynet ikke har ført et risikobaseret tilsyn. Datatilsynet har ikke udarbejdet selvstændige analyser af, hvilke behandlinger af personoplysninger der er forbundet med en særlig risiko i forhold til overholdelsen af GDPR. Datatilsynet har ikke opdateret sin overordnede strategi siden 2015 og tilrettelægger derfor stadig sine tilsyn på baggrund af sin strategi, fra før GDPR blev gældende. Desuden har Datatilsynet ikke kunnet dokumentere, at de tilsyn, Datatilsynet har planlagt, er udvalgt ud fra en risikobetragtning. Det betyder samlet set, at det er usikkert, om Datatilsynet har anvendt de tilgængelige resurser til at føre tilsyn, der hvor risikoen er størst, og dermed har opnået den størst mulige effekt af de midler, Datatilsynet har til rådighed.

Undersøgelsen viser også, at Datatilsynet kun har afsluttet 22 tilsyn, siden GDPR blev gældende, heraf vedrører 8 offentlige myndigheder og 14 private virksomheder. De 8 afsluttede tilsyn dækker en meget lille andel af de offentlige myndigheder. De få afsluttede tilsyn, siden GDPR blev gældende, betyder, at der er færre afgørelser og dermed et manglende fortolkningsbidrag til databeskyttelsesreglerne, som offentlige myndigheder kan rette sig efter med henblik på at sikre overholdelse af databeskyttelsesreglerne. Det betyder også, at den præventive effekt af Datatilsynets tilsynsaktivitet kunne have været større.

Datatilsynet har afsluttet 11 af sine 85 planlagte tilsyn. Hvis Datatilsynet havde opfyldt sit eget mål om at afslutte 80 % af sine tilsyn inden for 6 måneder, kunne Datatilsynet have afsluttet mindst 50 planlagte tilsyn inden udgangen af 2019.

Rigsrevisionen, den 6. maj 2020

Lone Strøm

/Michala Krakauer

Bilag 1. Metodisk tilgang

Formålet med undersøgelsen er at vurdere, om myndighederne har ydet en tilfredsstillende indsats for at sikre, at outsourcede følsomme og fortrolige persondata om borgerne opbevares sikkert. Derfor har vi undersøgt følgende:

- Har myndighederne haft en tilfredsstillende styring af databehandlere, som opbevarer følsomme eller fortrolige persondata?
- Har Justitsministeriet, herunder Datatilsynet, og Finansministeriet i tilstrækkelig grad understøttet de øvrige myndigheders styring af databehandlere?

I undersøgelsen indgår 17 ministerier og Region Midtjylland. Udenrigsministeriet indgår ikke i undersøgelsen, da ministeriet har oplyst, at ministeriet ikke har outsourcet opbevaringen af følsomme eller fortrolige persondata. For de 17 ministerier indgår kun myndigheder, hvor ministeren har instruktionsbeføjelse, hvilket typisk er departementer og styrelser. Vi har valgt at inddrage det regionale niveau i form af Region Midtjylland. Region Midtjylland adskiller sig ikke umiddelbart fra de andre regioner på parametre som typen af følsomme og fortrolige persondata, typer af databehandlinger o.l. Vi har inkluderet en region, fordi regionerne håndterer store mængder følsomme personoplysninger fra sundhedssektoren. I valget af region har vi desuden lagt vægt på, at Datatilsynet ikke inden for de seneste år havde ført tilsyn med regionen med fokus på samme tema, som denne undersøgelse.

Undersøgelsesperioden går fra april 2016, hvor GDPR blev vedtaget i EU, til den 1. januar 2020, hvor vi afsluttede vores materialeindsamling.

Kvalitetssikring

Denne undersøgelse er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos de reviderede samt ledelsesbehandling og sparring på forskellige tidspunkter i undersøgelsesforløbet med chefer og medarbejdere i Rigsrevisionen med relevante kompetencer.

Møder

Vi har holdt møder med alle ministerier og regioner. Formålet med møderne har været at drøfte undersøgelsens formål og metode.

Vi har løbende holdt møder med Datatilsynet om undersøgelsens relation til databeskyttelsesreglerne. Vi har desuden holdt møder med Digitaliseringsstyrelsen om arbejdet med at implementere ISO 27001 og med Statens It om overblik over it-systemer i staten og ansvarsfordelingen mellem Statens It og de enkelte ministerier, når Statens It er databehandler.

Derudover har vi holdt møder med en række interessenter på området i form af Bech Bruun, Kammeradvokaten, Djøfs TechDK Kommissionen, REVI-IT og IT-branchen. Formålet med møderne har været at få baggrundsinformation om området og et indblik i, hvordan erhvervslivet og offentlige myndigheder har tacklet databeskyttelsesreglerne, herunder særligt implementeringen af GDPR.

Vi har desuden holdt møde med Roskilde Kommune for at blive klogere på, hvordan kommuner går til styringen af databehandlere, og for at høre nærmere om tabet af dokumenter for 80.000 borgere i 2018.

Endelig har vi holdt møde med Hanne Marie Motzfeldt, lektor i digital forvaltning på Københavns Universitet, og Henrik Udsen, professor i it-ret på Københavns Universitet, for at få en dybere forståelse af GDPR's betydning for offentlige myndigheders styring af databehandlere.

Kapitel 2: Myndighedernes styring af databehandlere

Væsentlige dokumenter

Vi har gennemgået en række dokumenter fra myndighederne, herunder:

- lovgivning om databeskyttelse, herunder GDPR (databeskyttelsesforordningen) med virkning fra den 25. maj 2018, databeskyttelsesloven med virkning fra den 25. maj 2018 og persondataloven med virkning fra 2000, som implementererede databeskyttelsesdirektivet fra 1995 i Danmark
- risikovurderinger
- databehandleraftaler og øvrigt aftalegrundlag
- tilsynsplaner
- revisorerklæringer og anden dokumentation for gennemførte tilsyn
- mailkorrespondance, notater og mødereferater.

Udvælgelse af it-systemer

Formålet med gennemgangen af de outsourcede it-systemer, som opbevarer følsomme eller fortrolige personoplysninger, er at undersøge myndighedernes overordnede styring af databehandlere.

Vi bad i forbindelse med undersøgelsen alle ministerier og Region Midtjylland om at indsende en bruttoliste over outsourcede it-systemer, som opbevarede følsomme og/eller fortrolige persondata. Vi bad i første omgang myndighederne om at udfylde et skema for alle deres systemer med persondata og give ca. 20 grundoplysninger om hvert system, fx typer af persondata og oplysninger om databehandler og eventuelle underdatabehandlere. På baggrund af anmodningen meldte en række ministerier tilbage, at anmodningen ville medføre et meget betragteligt resursetræk, som ikke stod mål med formålet. Det er vores opfattelse, at myndigheder bør have et overblik over deres it-portefølje, som gør det muligt at besvare en sådan anmodning med et begrænset resurseforbrug. Da det for flere myndigheder ikke var tilfældet, bad vi i stedet myndighederne angive følgende for hvert system:

- systemnavn
- dataansvarlig myndighed
- systemets nøglefunktion
- eventuelle kommentarer.

På den baggrund sendte myndighederne oplysninger om ca. 950 it-systemer, som levede op til undersøgelsens afgrænsning. Vi udtog på baggrund af bruttolisten 10 systemer fra hvert ministerområde inkl. 2 systemer, hvor Statens It var databehandler, og 10 systemer fra Region Midtjylland. Hvis myndighederne havde færre end 10 systemer, som var omfattet af undersøgelsens afgrænsning, udtog vi alle deres systemer, men stadig højst 2 systemer, hvor Statens It var databehandler. Vi har valgt et begrænset antal systemer, hvor Statens It er databehandler, da databehandlerkonstruktionerne og aftalegrundlaget er ens i de fleste tilfælde, og Finansministeriet fører tilsyn med Statens It på vegne af de andre statslige myndigheder. For systemer, hvor Statens It er databehandler, har vi ikke udtaget systemer på driftsmodel 1, men kun systemer inden for driftsmodellerne 1a, 2, 2a, 3 og 5. Det skyldes, at ansvaret for systemer på driftsmodel 1 kun ligger hos Statens It. Vi har undersøgt, om Finansministeriet har ført tilsyn med Statens It og Statens Administration. Ligesom det er tilfældet for de øvrige tilsyn, har vi ikke vurderet, om indholdet af tilsynet har været tilstrækkeligt.

På baggrund af bruttolisten udvalgte vi i første omgang 158 it-systemer til undersøgelsen. I 35 tilfælde fandt myndighederne efter udvælgelsen ud af, at systemet alligevel ikke levede op til undersøgelsens afgrænsning. Det var fx tilfælde, hvor systemet slet ikke opbevarede persondata, hvor der ikke var tale om følsomme eller fortrolige persondata, eller hvor myndigheden ikke var dataansvarlig for de persondata, der var i systemet. I disse tilfælde udvalgte vi som udgangspunkt andre systemer som erstatning. I en række tilfælde modtog vi imidlertid nye oplysninger så sent i forløbet, at vi ikke erstattede systemerne. På den baggrund har vi undersøgt i alt 148 systemer.

Udvælgelsen af it-systemerne var baseret på en risikobetragtning. Vi har valgt en risikobaseret tilgang til udvælgelsen, fordi vi vurderer, at det er mere væsentligt at undersøge de mest risikofyldte systemer end at kunne generalisere til alle outsourcede systemer, som opbevarer følsomme eller fortrolige persondata. I vores udvælgelse tog vi højde for myndighedernes egne oplysninger om systemets funktion, det formodede omfang af personoplysninger og typer af data. Vi lagde også vægt på at variere på underliggende myndigheder inden for ministerområderne og typen af systemer for at favne så bredt som muligt. Typen af systemer kan fx omfatte journalsystemer, registre og sagsbehandlingssystemer.

Vi har afgrænset os fra it-systemer, som var under udfasning eller var genstand for selvstændige undersøgelser fra Rigsrevisionen. Vi har desuden afgrænset os fra fællesstatslige it-systemer, hvor kun én central myndighed er dataansvarlig.

Gennemgang af it-systemer
Vi har gennemgået 22 spørgsmål for de 148 it-systemer. Spørgsmålene er fordelt på 3 temaer: risikovurderinger, databehandleraftaler og tilsyn. Tilsyn omfatter også spørgsmål vedrørende brugen af underdatabehandlere. Hvert spørgsmål har en række udfaldsrum. Vi bad i første omgang ministerierne angive det udfaldsrum, som de vurderede var mest retvisende, og medsende dokumentation herfor. Efterfølgende har vi gennemgået myndighedernes svar og dokumentation for alle systemerne. For at sikre en ensartet vurdering på tværs af systemerne er alle systemer gennemgået af mindst 2 fra projektgruppen. Alle tvivlsspørgsmål er drøftet i hele projektgruppen, og vi har genbesøgt mange af vores vurderinger undervejs i undersøgelsen for at sikre validiteten og konsistensen af vurderingerne på tværs af systemer. Efterfølgende har myndighederne haft mulighed for at kommentere på vores vurderinger og sende supplerende materiale i deres høringssvar, som vi har taget i betragtning i vores endelige vurderinger.

Vi har kun vurderet spørgsmålene på baggrund af skriftlig dokumentation. Det er Rigsrevisionens opfattelse, af det er udtryk for god styring hos offentlige myndigheder, at overvejelser og beslutninger i henhold til databeskyttelse dokumenteres skriftligt. Det skyldes, at det fx for risikovurderinger er væsentligt for myndighederne senere at kunne genbesøge risikovurderingerne, når de skal føre tilsyn, genforhandle databehandleraftaler e.l., ligesom skriftlighed vil sikre ensartethed på tværs af risikovurderingerne. Samtidig stiller GDPR krav til, at myndigheder i højere grad end tidligere skal dokumentere deres overvejelser i forhold til overholdelse af databeskyttelsesreglerne.

Vi har sat skæringsdatoer for, hvornår dokumentationen skal have været udarbejdet, for at vi tager det i betragtning i undersøgelsen. Det skyldes hensynet til, at resultaterne skal illustrere situationen på det tidspunkt, hvor vi indsamlede materiale. For risikovurderinger og databehandleraftaler har vi sat skæringsdatoen til den 20. september 2019, som var den dato, hvor myndighederne skulle fremsende materiale for systemerne. For tilsynsaktiviteter har vi sat skæringsdatoen til den 20. august 2019, hvor vi fremsendte materialeanmodningen til myndighederne. Forskellen skyldes, at risikovurderinger og databehandleraftaler ofte har længere forløb, og at myndighederne skulle have mulighed for at afslutte igangværende arbejde. Flere tilsynsaktiviteter, fx at indhente en generel revisorerklæring eller stille opfølgende spørgsmål til en databehandler, kan gøres med en relativt kort tidsfrist. Vi har derfor vurderet, at det vil give det mest retvisende billede, uafhængigt af undersøgelsen, at tilsynsaktiviteter og godkendelse af underdatabehandlere skulle være udført inden fremsendelsen af materialeanmodningen.

For visse spørgsmål, fx datas faktiske fysiske placering og adgang til data fra tredjelande, har vi baseret os på skriftlige oplysninger fra databehandlere og ikke fra myndighederne selv. Af tabel A fremgår de 22 spørgsmål, som vi har gennemgået for alle 148 it-systemer. Af tabellen fremgår også de mulige udfaldsrum og kriterier, som vi har lagt til grund for vores vurderinger og konklusioner. For figur 9 om kendskab til alle underdatabehandlere gør det sig gældende, at spørgsmålet ikke fremgår eksplicit af kodebogen. Figuren er baseret på data fra spørgsmål 3.e om godkendelse af underdatabehandlere.

Tabel A

Kodebog

Tema 1: Risikovurderinger

Spørgsmål	Udfaldsrum	Kriterier
1.a) Er der udarbejdet en risikovurdering?	I. Ja	Der foreligger et skriftligt dokument, som forholder sig til "risici" i forhold til det specifikke system eller den behandling, der er knyttet til det specifikke system.
	II. Nej	Der foreligger *ikke* et skriftligt dokument, som forholder sig til "risici" i forhold til det specifikke system eller den behandling, der er knyttet til det specifikke system.
1.b) Risikovurderingens dato	I. [dato]	Dato for, hvornår risikovurderingen er færdiggjort/underskrevet.
1.c) Ligger risikovurderingen forud for databehandleraftalen?	I. Ja	Risikovurderingen er færdiggjort forud for, at databehandleraftalen er indgået. Der er få tilfælde, hvor en risikovurdering er udarbejdet over flere måneder og er endeligt godkendt kort tid efter databehandleraftalen. I de tilfælde har vi kodet "ja", hvor der foreligger dokumentation for, at udarbejdelsen af risikovurderingen er påbegyndt inden eller foregået i forbindelse med udarbejdelsen af databehandleraftalen.
	II. Nej	Risikovurderingen er færdiggjort, efter databehandleraftalen er indgået.
1.d) Forholder risikovurderingen sig til risici for de registreredes rettigheder?	I. Ja	Risici eller konsekvenser for de registrerede rettigheder nævnes eksplicit i risikovurderingen. Det er ikke tilstrækkeligt, at der fx nævnes omfanget eller typen af persondata, hvis ikke det sættes i kontekst til de risici eller konsekvenser, det kan have for de registrerede ved fx databrud eller uvedkommendes adgang til data.
	II. Nej	Risici eller konsekvenser for de registrerede rettigheder nævnes *ikke* eksplicit i risikovurderingen.
1.e) Indeholder risikovurderingen overvejelser om konsekvens og sandsynlighed?	I. Ja	Risikovurderingen indeholder både en vurdering af sandsynligheden for, at sikkerhedshændelser sker, og konsekvensen af sådanne sikkerhedshændelser.
	II. Nej	Risikovurderingen indeholder en vurdering af sandsynlighed eller konsekvens eller ingen af delene.
Tema 2: Databehandleraftaler		
2.a) Er der indgået en databehandleraftale?	I. Ja	Der eksisterer en skriftlig databehandleraftale, som omhandler det specifikke system, og hvor navnet på den dataansvarlige og databehandleren fremgår. Hvis der i aftalen er krav om begge parters underskrift, før aftalen er gældende, vurderer vi kun, at den er gældende, hvis både den dataansvarlige og databehandleren har underskrevet aftalen. Vi kontrollerer ikke, om indholdet af databehandleraftalen lever op til GDPR. Vi er stødt på enkelte tilfælde, hvor der ikke foreligger en gyldig databehandleraftale, men hvor myndigheden har en kontrakt eller andet aftalegrundlag, som i et vist omfang regulerer forholdet mellem den dataansvarlige og databehandleren.
	II. Nej	Der eksisterer *ikke* en skriftlig databehandleraftale, som omhandler det specifikke system, eller aftalen er ikke underskrevet, selv om der i aftalen er krav om underskrift.
	III. Databehandleraftalen er under udarbejdelse	Der eksisterer ikke en skriftligt databehandleraftale, men myndigheden oplyser, at den er under udarbejdelse.
2.b) Databehandleraftalens dato	I. [dato]	Dato for databehandleraftalens ikrafttræden eller dato for sidste underskrift, hvis der er krav om underskrift.
2.c) Er der taget stilling til datas fysiske opbevaring?	I. Ja	Datas fysiske placering er beskrevet i aftalen. Det kan enten være, at data *skal* opbevares i et bestemt land eller en bestemt region eller *ikke må* forlade et bestemt land eller en bestemt region.
	II. Nej	Datas fysiske placering er ikke beskrevet i aftalen, eller der er ikke en gældende databehandleraftale.

Spørgsmål	Udfaldsrum	Kriterier
2.d) Hvor skal data fysisk opbevares?	I. [geografisk lokalitet]	Land/område, hvor data ifølge aftalen skal opbevares, eller land/område, som data ikke må forlade, fx EU/EØS.
2.e) Hvor var data fysisk opbevaret kl. 12.00 den 1. august 2019?	I. [geografisk lokalitet]	Land/område, hvor data fysisk blev opbevaret den 1. august 2019 kl. 12.00. Kræver et svar fra databehandleren, fx i form af en mail. Kræver ikke log e.l.
	II. Kan ikke dokumenteres	Databehandleren har ikke kunnet oplyse, hvor data blev fysisk opbevaret den 1. august 2019 kl. 12.00.
2.f) Har personer fra sikre/usikre tredjelande eller internationale organisationer haft adgang til at behandle data (herunder "se-adgang") inden for det seneste år (1. august 2018 - 31. juli 2019)?	Én eller flere af følgende valgmuligheder:	
	I. Personer fra usikre tredjelande	Databehandleren oplyser, at personer fra usikre tredjelande har haft adgang til persondata. Dette gælder også for cloud-systemer, hvor der *kan* have været adgang til persondata fra usikre tredjelande, men hvor det ikke kan afgøres, om der i praksis har været adgang.
	II. Personer fra sikre tredjelande	Databehandleren oplyser, at personer fra sikre tredjelande har haft adgang til persondata. Dette gælder også for cloud-systemer, hvor der *kan* have været adgang til persondata fra sikre tredjelande, men hvor det ikke kan afgøres, om der i praksis har været adgang.
	III. Personer fra internationale organisationer	Databehandleren oplyser, at personer fra internationale organisationer har haft adgang til persondata. Dette gælder også for cloud-systemer, hvor der *kan* have været adgang til persondata fra internationale organisationer, men hvor det ikke kan afgøres, om der i praksis har været adgang.
	IV. Ingen personer fra sikre/usikre tredjelande eller internationale organisationer	Databehandleren oplyser, at ingen personer fra sikre/usikre tredjelande eller internationale organisationer har haft adgang til persondata.
	V. Kan ikke dokumenteres	Databehandleren kan eller ønsker ikke at oplyse, om der har været adgang til persondata fra sikre/usikre tredjelande eller internationale organisationer.
2.g) Hvis ja, hvor har personer med adgang været fysisk placeret?	[geografisk lokalitet]	Land/område, hvor personer har haft adgang til persondata.
2.h) Hvilke typer af tilsyn kan den dataansvarlige føre med databehandleren?	Én eller flere af følgende valgmuligheder:	
	I. Fysisk tilsyn	Det fremgår af databehandleraftalen, at den dataansvarlige har adgang til fysiske inspektioner hos databehandleren.
	II. Indhente relevante oplysninger	Det fremgår af databehandleraftalen, at databehandleren skal stille oplysninger til rådighed for den dataansvarlige.
	III. Indhente generel revisorerklæring	Det fremgår af databehandleraftalen, at en uafhængig revisor har mulighed for at efterse databehandlerens generelle interne styring og kontroller. Hvis ikke det er nærmere specificeret, om der er tale om en generel eller specifik revisorerklæring, har vi vurderet, at der som udgangspunkt er mulighed for at indhente begge typer revisorerklæringer.
	IV. Indhente specifik revisorerklæring	Det fremgår af databehandleraftalen, at en uafhængig revisor har mulighed for at efterse overholdelsen af databehandleraftalen. Hvis ikke det er nærmere specificeret, om der er tale om en generel eller specifik revisorerklæring, har vi vurderet, at der som udgangspunkt er mulighed for at indhente begge typer revisorerklæring.
	V. Der er ikke mulighed for at føre tilsyn	Der er enten ikke nogen databehandleraftale, eller muligheden for tilsyn er ikke specificeret i databehandleraftalen.
	VI. Finansministeriet fører tilsyn	Gælder for systemer, hvor Statens It eller Statens Administration er databehandler, da Finansministeriet fører et årligt tilsyn med Statens It og Statens Administration.

Spørgsmål	Udfaldsrum	Kriterier
2.i) Er der taget stilling til godkendelse af underdatabehandlere?	I. Brug af underdatabehandlere skal specifikt godkendes	Det fremgår af databehandleraftalen, at myndigheden skal godkende underdatabehandlere, inden databehandleren må benytte dem.
	II. Der er givet generel godkendelse til brug af underdatabehandlere	Det fremgår af databehandleraftalen, at databehandleren har myndighedens generelle tilladelse til at benytte underdatabehandlere, og at myndigheden ikke specifikt skal godkende underdatabehandlerne, inden databehandleren tager dem i brug. Typisk skal myndigheden dog orienteres og vil som hovedregel have mulighed for at gøre indsigelser over for valget af konkrete underdatabehandlere.
	III. Der er ikke taget stilling til godkendelse af underdatabehandlere	Enten findes der ikke en gældende databehandleraftale, eller brugen af underdatabehandlere er ikke specificeret i databehandleraftalen.
2.j) Skal underdatabehandlere overholde samme sikkerhedskrav som databehandleren?	I. Ja	Det fremgår af databehandleraftalen, at eventuelle underdatabehandlere skal overholde de sikkerhedskrav, som er specificeret i databehandleraftalen mellem den dataansvarlige og databehandleren.
	II. Nej	Enten findes der ikke en gældende databehandleraftale, eller det fremgår *ikke* af databehandleraftalen, at eventuelle underdatabehandlere skal overholde de sikkerhedskrav, som er specificeret i databehandleraftalen mellem den dataansvarlige og databehandleren.
2.k) Skal der indgås en databehandleraftale mellem databehandleren og underdatabehandlere?	I. Ja	Det fremgår af databehandleraftalen, at brugen af eventuelle underdatabehandlere skal reguleres ved en skriftlig aftale mellem databehandleren og underdatabehandlere.
	II. Nej	Enten findes der ikke en gældende databehandleraftale, eller det fremgår *ikke* af databehandleraftalen, at brugen af eventuelle underdatabehandlere skal reguleres ved en skriftlig aftale mellem databehandleren og underdatabehandlere.
Tema 3: Tilsyn		
3.a) Er der en plan for, hvornår og hvordan der skal føres tilsyn med databehandleren?	I. Der findes en plan for at føre tilsyn	Der findes et skriftligt dokument, som beskriver, hvordan og hvor ofte der skal føres tilsyn med det specifikke system. Det kan fx være en bestemmelse i databehandleraftalen eller et selvstændigt dokument.
	II. Der findes en overordnet tilsynsplan i myndigheden	Der findes et skriftligt dokument, som beskriver, hvordan myndigheden generelt skal føre tilsyn med databehandlere, men det er ikke specificeret, hvordan eller hvor ofte der skal føres tilsyn med det specifikke system.
	III. Der findes ikke en plan for at føre tilsyn	Der findes ikke et skriftligt dokument, som enten beskriver, hvordan myndigheden generelt skal føre tilsyn, eller hvordan der skal føres tilsyn med det specifikke system.
	IV. Finansministeriet fører tilsyn	Gælder for systemer, hvor Statens It eller Statens Administration er databehandler, da det er Finansministeriets ansvar at føre et årligt tilsyn med Statens It og Statens Administration.

Spørgsmål	Udfaldsrum	Kriterier
3.b) Er der ført tilsyn med databehandleren (efter databehandleraftalen er indgået)?	Én eller flere af følgende valgmuligheder:	
	I. Der er indhentet relevante oplysninger	Myndigheden har indhentet relevante oplysninger fra databehandleren uafhængigt af en specifik eller generel revisorerklæring. Det kan fx være mailkorrespondance med spørgsmål om databehandling, indhentning af databehandleraftaler med underdatabehandlere og telefonnotat.
	II. Der er ført eget fysisk tilsyn	Myndigheden har ført eget fysisk tilsyn med databehandleren uafhængigt af en specifik eller generel revisorerklæring. Det kan typisk dokumenteres ved mailkorrespondance, internt notat, mødereferat mv.
	III. Der er indhentet en generel revisorerklæring	Myndigheden har indhentet en generel revisorerklæring, som omhandler databehandleren. En generel revisorerklæring kigger som udgangspunkt på databehandlerens generelle it-sikkerhed, interne kontroller og i nogle tilfælde databeskyttelse. Denne type erklæring kigger som udgangspunkt ikke på det specifikke system eller den behandling, der er knyttet til systemet.
	IV. Der er indhentet en specifik revisorerklæring	Myndigheden har indhentet en specifik revisorerklæring, som omhandler det specifikke system. En specifik revisorerklæring omfatter det specifikke system eller den databehandling, som myndigheden har outsourcet.
	V. Finansministeriet har ført tilsyn	Gælder for systemer, hvor Statens It eller Statens Administration er databehandler, da Finansministeriet fører et årligt tilsyn med Statens It og Statens Administration.
	VI. Der er ikke ført tilsyn	Myndigheden har ikke ført et tilsyn eller har ikke kunnet dokumentere, at der er ført tilsyn med databehandleren.
3.c) Dato for senest udførte tilsyn	I. [dato]	Dato for det senest udførte tilsyn.
3.d) Er der fulgt op på tilsynet?	I. Ja	Skriftlig dokumentation for, at myndigheden har taget stilling til resultaterne af det gennemførte tilsyn. Det kan fx være et internt opfølgningsnotat, mødereferat og mailkorrespondance med databehandleren.
	II. Nej	Der er ikke skriftlig dokumentation for, at myndigheden har taget stilling til resultaterne af det gennemførte tilsyn.
3.e) Er underdatabehandlere specifikt eller generelt godkendt?	I. Der er givet specifik godkendelse af alle underdatabehandlere	Skriftlig dokumentation for, at myndigheden specifikt har godkendt alle underdatabehandlere, som databehandleren skriftligt oplyser, at der gøres brug af. Det kan fx være i mailkorrespondance, mødereferater og databehandleraftalen. Kræver, at der i databehandleraftalen er stillet krav om specifik godkendelse.
	II. Der er givet specifik godkendelse af nogle af underdatabehandlerne	Skriftlig dokumentation for, at myndigheden specifikt har godkendt nogle, men ikke alle, underdatabehandlere, som databehandleren skriftligt oplyser, at der gøres brug af. Det kan fx være i mailkorrespondance, mødereferater og databehandleraftalen. Kræver, at der i databehandleraftalen er stillet krav om specifik godkendelse.
	III. Der er givet generel godkendelse, og myndigheden er blevet underrettet om brug af alle underdatabehandlere	Skriftlig dokumentation for, at myndigheden er blevet orienteret om alle underdatabehandlere, som databehandleren skriftligt oplyser, at der gøres brug af. Det kan fx være i mailkorrespondance og mødereferater. Kræver, at der er givet generel godkendelse i databehandleraftalen.
	IV. Der er givet generel godkendelse, og myndigheden er blevet underrettet om brug af nogle af underdatabehandlerne	Skriftlig dokumentation for, at myndigheden er blevet orienteret om nogle, men ikke alle, underdatabehandlere, som databehandleren skriftligt oplyser, at der gøres brug af. Det kan fx være i mailkorrespondance og mødereferater. Kræver, at der er givet generel godkendelse i databehandleraftalen.
	V. Der er givet generel godkendelse, men myndigheden er ikke blevet underrettet om brug af underdatabehandlere	Der er ikke skriftlig dokumentation for, at myndigheden er blevet orienteret om nogen af de underdatabehandlere, som databehandleren skriftligt oplyser, at der gøres brug af.

Spørgsmål	Udfaldsrum	Kriterier
	VI. Der er hverken givet specifik eller generel godkendelse til brug af underdatabehandlere	Databehandleren har oplyst, at der benyttes underdatabehandlere, men der er enten ikke en databehandleraftale, eller brugen af underdatabehandlere er ikke reguleret i databehandleraftalen.
	VII. Databehandleren benytter ikke underdatabehandlere	Skriftlig dokumentation fra databehandleren for, at databehandleren ikke benytter underdatabehandlere.
3.f) Er der ført tilsyn med underdatabehandlere?	I. Der er ført tilsyn med alle underdatabehandlere	Skriftlig dokumentation for, at der er ført tilsyn med alle oplyste underdatabehandlere. Kan fx være revisorerklæringer og databehandlerens eget tilsyn.
	II. Der er ført tilsyn med nogle af underdatabehandlerne	Skriftlig dokumentation for, at der er ført tilsyn med nogle, men ikke alle, oplyste underdatabehandlere. Kan fx være revisorerklæringer, databehandlerens eget tilsyn eller indhentning af oplysninger.
	III. Tilsyn med underdatabehandlere er ud fra en risikobetragtning fravalgt	Skriftlig dokumentation for, at tilsyn med underdatabehandlere er fravalgt ud fra en risikobetragtning. Kan fx være mailkorrespondance og telefonnotater fra dialog med databehandlere.
	IV. Der er planlagt tilsyn, som endnu ikke er udført	Skriftlig dokumentation for, at der er planer om at gennemføre et tilsyn med underdatabehandlere, som endnu ikke er udført.
	V. Der er ikke ført tilsyn med underdatabehandlere	Der er ikke skriftlig dokumentation for, at der er udført eller planlagt tilsyn med nogen underdatabehandlere.
	VI. Databehandleren benytter ikke underdatabehandlere	Skriftlig dokumentation fra databehandleren for, at databehandleren ikke benytter underdatabehandlere.

Vi har undersøgt i alt 148 it-systemer. De undersøgt systemer og den dataansvarlige myndighed fremgår af tabel B.

Tabel B

Oversigt over de 148 it-systemer i undersøgelsen

Ministerium/region og dataansvarlig myndighed	Systemnavn
Beskæftigelsesministeriet:	
Arbejdstilsynet	• ATIS • Blanketmotor • Damvad analysesystem
Departementet	• Refusionssystemet • Fleks- og barselsordninger TMO
Styrelsen for Arbejdsmarked og Rekruttering	• DenDigitaleJobBro.dk • VAS • DFDG • Udvikling i fleksjob II • Manuscript
Børne- og Undervisningsministeriet:	
Styrelsen for It og Læring	• Trivselsmålingsværktøj • Insubiz • SPS 2005 • PULS • Public360
Erhvervsministeriet:	
Erhvervsstyrelsen	• Kontrol OG Tilsyn (KOGT) 2019 • Straffeattestkomponent • Hvidvask • Frakendelsesregisteret
Finanstilsynet	• Remote Backup • Digital Post
Konkurrence- og Forbrugerstyrelsen	• Whistleblower-system
Nævnenes Hus	• Public 360
Patent- og Varemærkestyrelsen	• TSM backup
Sikkerhedsstyrelsen	• Workzone
Finansministeriet:	
Digitaliseringsstyrelsen	• NemID (RID og PID nummer) • Borger.dk support løsning • NemKonto inkl. Ventekonto • Digital Post (Digitaliseringsstyrelsen som offentlig afsender) • Borger.dk
Moderniseringsstyrelsen	• Statens Lønsystem (SLS) inkl. Statens Pensionssystem (SP) • Tribis Integration Engine • Mercell
Statens Administration	• TMO (refusion flexjob og barsel) • Lønportalen (blanketløsningen)

Ministerium/region og dataansvarlig myndighed	Systemnavn
Forsvarsministeriet:	
Forsvarsministeriets Personalestyrelse	• Xform • NOVAX Session
Beredskabsstyrelsen	• SurveyXact • Novax A/S
Forsvarsakademiet	• Post-Let
Departementet	• DeMars • KESDH
Forsvarets Sanitetskommando	• Webreq
Forsvarsministeriets Materiel- og Indkøbsstyrelse	• Opbevaringstjeneste Juridisk servicebureau Aps.
Justitsministeriet:	
Departementet	• Whistleblowerportal
Kriminalforsorgen	• Radikaliserings Indberetnings System (RIS) • Elektronisk overvågning af klienter i fodlænke (Intensiv overvågning (IO) (Fodlænke)) • POM • XMO • Backup
Civilstyrelsen	• JIF-Extranet
Rigspolitiet	• Index 1 • PAS • Kriminalregisteret
Kirkeministeriet:	
Departementet	• SBL • IHLP • Person og Selvbetjeningsløsninger • Kandidatsystem • Kompetenceløft • Kompetencefond • Acadre • KIS (Kirkenettets Informationssystem) • F2
Klima-, Energi- og Forsyningsministeriet:	
Geodatastyrelsen	• Målebladsarkiv Danmark
Energistyrelsen	• Selvbetjeningsportalen for solpuljerne • PANDA • Easy Energy • Tilsynsdatabasen – Frekvensregistret • Doc2Archive
De Nationale Geologiske Undersøgelser for Danmark og Grønland	• Outlook i Office 365
Danmarks Meteorologiske Institut	• mTime
Styrelsen for Dataforsyning og Effektivisering	• Datafordeleren

Ministerium/region og dataansvarlig myndighed	Systemnavn
Kulturministeriet:	
Slots- og Kulturstyrelsen	• X-form (Capevo) • Digital Post • FilArkiv • SurveyXact
Det Danske Filminstitut	• Journalen
Rigsarkivet	• Sofia-oparbejdning
Miljø- og Fødevareministeriet:	
Departementet	• Ennova A/S • Digital Post
Fiskeristyrelsen	• BTAS
Landbrugsstyrelsen	• CAP-TAS
Fødevarestyrelsen	• GLR/CHR • VETREG • VETSTAT
Naturstyrelsen, Kystdirektoratet	• Public 360
Region Midtjylland:	
	• EG Sensum Bosted • EDI • Emento (Digital forløbsguide) • InfCare • OpenTele • PPJ • Notus Suite Maintenance • IBI (Interregionalt billedindeks) • Patobank • Sårjournalen
Skatteministeriet:	
Skatteforvaltningen	• Tast Selv Borger – Forskud • office365 inkl. Azure • Datawarehouse • Tast Selv Borger – Årsopgørelsen • Centrale Skatteyder Register – Persondelen • Debitor og Restancesystem • A-Kasse bidrag og Faglige kontingenter • Centrale Oplysningsseddel Register • Centrale Pensions System (CPS)
Spillemyndigheden	• Register Over Frivilligt Udelukkede Spillere

Ministerium/region (dataansvarlig myndighed)	Systemnavn
Social- og Indenrigsministeriet:	
Departementet	• Digitale Vælgererklæringer • Qlik Sense (Click Sense)
Familieretshuset	• F2 • Oracle DB
Socialstyrelsen	• F2 • MyClinic
Ankestyrelsen	• Anker – sagssortering • Public 360
CPR-administrationen	• Forskerudtræk • CPR-systemet
Statsministeriet:	
Departementet	• Digital Post • F2-ESDH • FERIEBEREGNING-DB
Sundheds- og Ældreministeriet:	
Lægemiddelstyrelsen	• Sentinel (MHRA)
Statens Serum Institut	• Elektronisk arkiv hos Larix • Computerrome
Styrelsen for Patientsikkerhed	• Dansk Patientsikkerhedsdatabase
Sundhedsdatastyrelsen	• SEI2 • LPR3 • National Service Platform • Fælles Medicinkort (FMK) • Organdonorregister
Sundhedsstyrelsen	• Styrket Rehabiliteringsindsats for de svageste ældre
Transport- og Boligministeriet:	
Banedanmark	• Sharepoint Online • Whistleblower
Bygningsstyrelsen	• Public 360 • Targit
Havarikommissionen for Civil Luftfart og Jernbane	• F2
Trafik-, Bygge- og Boligstyrelsen	• SurveyXact
Uddannelses- og Forskningsministeriet:	
Styrelsen for Institutioner og Uddannelsesstøtte	• ekstranet.fi.dk • Public 360 • Digital post

Ministerium/region og dataansvarlig myndighed	Systemnavn
Udlændinge- og Integrationsministeriet	
Styrelsen for International Rekruttering og Integration	• VITAS • Gemini • Strålfors Connect • Keesing
Udlændingestyrelsen	• Keesing • Kortbestillingsløsning • Digital Post
Departementet/Udlændingestyrelsen/Udlændingenævnet/ Udenrigsministeriet/Rigspolitiet	• IVR-VIS
Udlændingestyrelsen/Styrelsen for International Rekruttering og Integration	• CARL2

Kapitel 3: Understøttelse af myndighedernes styring af databehandlere

Væsentlige dokumenter

Vi har i forbindelse med dette kapitel gennemgået en række dokumenter, herunder:

- lovgivning om databeskyttelse, herunder GDPR (databeskyttelsesforordningen) med virkning fra den 25. maj 2018, databeskyttelsesloven med virkning fra den 25. maj 2018 og persondataloven med virkning fra 2000, som implementererede databeskyttelsesdirektivet fra 1995 i Danmark
- vejledninger og skabeloner om databeskyttelse udgivet af Finansministeriet, Justitsministeriet og Datatilsynet
- strategier og tilsynsplaner om Datatilsynets tilsynsaktivitet
- data om Datatilsynets tilsynsaktivitet
- korrespondance mellem Finansministeriet, Datatilsynet og Justitsministeriet om udarbejdelse af vejledninger.

Formålet med gennemgangen af dokumenterne var at belyse Finansministeriets, Datatilsynets og Justitsministeriets vejledningsindsats samt Datatilsynets tilsynsindsats.

Spørgeskemaundersøgelse

Formålet med spørgeskemaundersøgelsen var at vurdere Digitaliseringsstyrelsens, Datatilsynets og Justitsministeriets vejledningsindsats i forbindelse med implementeringen af GDPR. Det er vores vurdering, at de enkelte myndigheder, som vejledningerne har været målrettet, har den bedste indsigt i, om vejledningsmaterialet har været brugbart. Vi har gennemført spørgeskemaundersøgelsen i form af et elektronisk spørgeskema.

Spørgeskemaundersøgelsen blev pilottestet hos en enkelt myndighed inden udsendelse og blev efterfølgende udsendt til 79 myndigheder medio september 2019 med en svarfrist på 2 uger. De 79 myndigheder er de myndigheder, som er dataansvarlige for it-systemer, som fremgik af ministeriernes og Region Midtjyllands indsendte bruttolister over outsourcede systemer, som opbevarede følsomme eller fortrolige persondata, uanset om myndighedernes systemer blev udvalgt blandt de 148 systemer i beretningens kapitel 2.

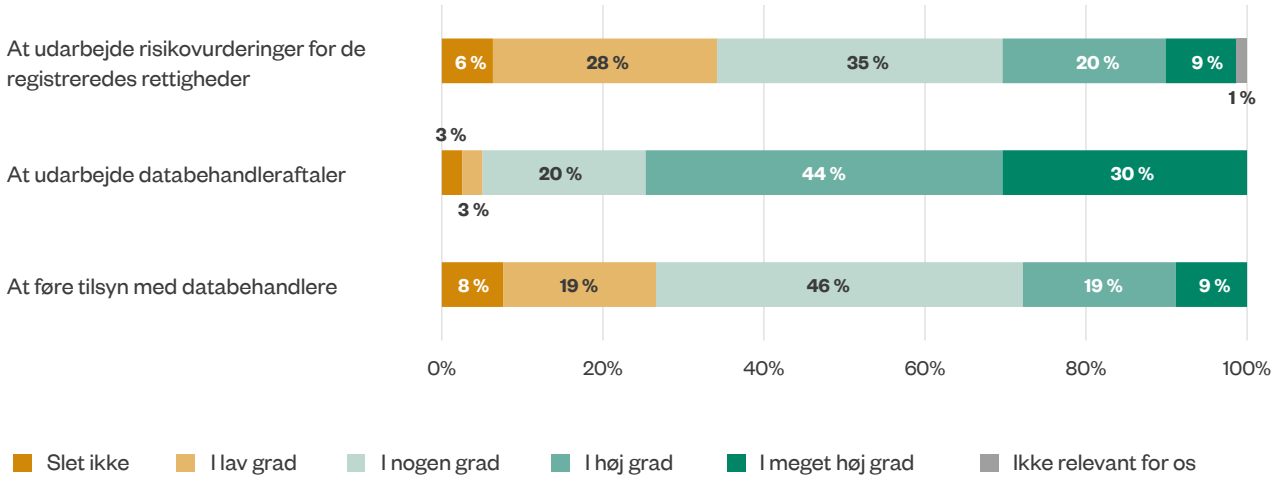
Svarprocenten på spørgeskemaundersøgelsen er 100 %. Spørgeskemaundersøgelsen bestod af 9 lukkede spørgsmål foruden spørgsmål til baggrundsinformation om myndighederne. Herudover indgik der 12 fritekstfelter. I det omfang besvarelser fra fritekstfelter er anvendt i beretningen, er det godkendt af de pågældende respondenter.

De følgende figurer viser resultaterne af spørgeskemaundersøgelsen for de lukkede spørgsmål, som afrapporteres i beretningen.

Figur A

Besvarelse af Rigsrevisionens spørgeskema i forhold til, om den samlede vejledningsindsats har understøttet myndighederne i arbejdet med at udarbejde risikovurderinger, indgå databehandleraftaler og føre tilsyn

I hvilken grad oplever I, at den samlede vejledning fra Justitsministeriet, Datatilsynet og Digitaliseringsstyrelsen har understøttet jer i følgende aktiviteter:



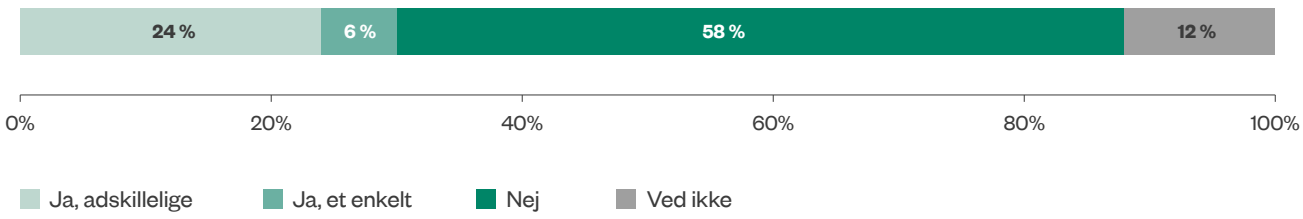
Note: n=79 myndigheder. På grund af afrundinger summerer risikovurderinger og tilsyn ikke til 100 %.

Kilde: Rigsrevisionens spørgeskemaundersøgelse.

Figur B

Besvarelse af Rigsrevisionens spørgeskema i forhold til, om myndighederne har igangsat initiativer, som kunne have været undgået

Har I iværksat initiativer (herunder købt privat rådgivning), som kunne være undgået, hvis vejledningsindsatsen havde været mere konkret eller mere omfangsrig, eller hvis vejledninger var udkommet tidligere?



Note: n=79 myndigheder.

Kilde: Rigsrevisionens spørgeskemaundersøgelse.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision. Standarderne fastlægger, hvad brugerne og offentligheden kan forvente af revisionen, for at der er tale om en god faglig ydelse. Standarderne er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).

Bilag 2. Ordliste

Ad hoc-tilsyn	Ad hoc-tilsyn er tilsyn, som iværksættes som følge af konkrete hændelser, fx medieomtale, klager eller anmeldelser.
Almindelige personoplysninger	Almindelige personoplysninger omfatter alle oplysninger, der ikke er kategoriseret som følsomme personoplysninger i GDPR, eller som opfattes som fortrolige oplysninger i en dansk kontekst. Se "Følsomme og fortrolige personoplysninger". Almindelige personoplysninger kan fx være navn og adresse eller generelle oplysninger om personlige økonomiske forhold.
Behandling af personoplysninger	Behandling af personoplysninger er et bredt begreb, som fx kan omfatte opbevaring, indsamling, registrering, organisering, systematisering, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse af personoplysninger.
Cloud-services	Cloud-services dækker bredt set over internetbaserede it-løsninger. Løsningerne kan have mange former – fra programmer som fx Gmail og Facebook, som tilgås via internettet og ikke er installeret på computeren, til løsninger, som kun opbevarer data. Opbevaringsløsningerne kan variere i fuldstændighed – fra færdige løsninger som fx Dropbox og Google Drive til mere rå serverkapacitet som fx Microsoft Azure og Amazon Web Service. Fælles for løsningerne er, at data og applikation ligger på internettet og ikke på den computer, som man tilgår løsningerne fra.
Dataansvarlig	Den juridiske eller fysiske person, private virksomhed, offentlige myndighed mv., der bestemmer, til hvilket formål og hvordan personoplysningerne må behandles.
Databehandler	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.
Databeskyttelsesdirektivet	Databeskyttelsesdirektivet er et tidligere EU-direktiv fra 1995 om behandlingen af personoplysninger, som blev indført i dansk lov ved persondataloven i 2000. Databeskyttelsesdirektivet blev i 2018 erstattet af GDPR (databeskyttelsesforordningen).
Databeskyttelsesloven	Databeskyttelsesloven (lov nr. 502 af 23. maj 2018) trådte i kraft samtidig med GDPR (25. maj 2018) og supplerer GDPR i en dansk kontekst. Databeskyttelsesloven indeholder bl.a. en bestemmelse om, hvilke systemer der *skal* opbevares i Danmark (lokationskravet), og fastsætter nærmere regler for Datatilsynets arbejde.
Fortrolige personoplysninger	Fortrolige oplysninger er en særlig kategori af personoplysninger, der ikke nævnes direkte af GDPR, men hvor der kan være særlige beskyttelsesbehov. Det er som udgangspunkt kontekstafhængigt, hvornår en oplysning opfattes som fortrolig, men databeskyttelsesloven fastslår, at cpr-numre og oplysninger om strafbare forhold (fx oplysninger om lovovertrædelser og politianmeldelse af borgeren) skal opfattes som fortrolige oplysninger i en dansk kontekst.
Fællesstatslige it-systemer	Fællesstatslige it-systemer er systemer, som én myndighed er ansvarlig for, men som benyttes af en lang række myndigheder på tværs af staten, fx Statens Budgetsystem og statens rejseafregnings- og udlægssystem (RejsUd). Typisk er den ansvarlige myndighed, og ikke de enkelte myndigheder, dataansvarlig for data, som behandles i systemet.

Følsomme personoplysninger	Følsomme personoplysninger defineres i GDPR's artikel 9 som personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssige tilhørsforhold samt behandling af genetiske data, biometriske data med det formål at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. Behandling af disse personoplysninger kræver en højere grad af beskyttelse end almindelige personoplysninger (se "Almindelige personoplysninger).
GDPR	Forkortelse for General Data Protection Regulation. Den danske oversættelse er databeskyttelsesforordningen.
Generel godkendelse af underdatabehandlere	Myndighederne kan i databehandleraftalen give databehandleren en generel godkendelse til at benytte underdatabehandlere. Det betyder, at databehandleren kan anvende nye underdatabehandlere uden en forudgående specifik godkendelse fra den dataansvarlige myndighed. Myndigheden skal dog underrettes om nye underdatabehandlere og kan eventuelt gøre indsigelser.
Generel revisorerklæring	En generel revisorerklæring omfatter som udgangspunkt databehandlerens generelle it-sikkerhed, interne kontroller og i nogle tilfælde databeskyttelse. Denne type erklæring omfatter som udgangspunkt ikke det specifikke system eller den behandling af persondata, som finder sted i systemet.
Informationssikkerhed	Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer mod at gå tabt eller falde i forkerte hænder. I arbejdet indgår bl.a. organisering af sikkerhedsarbejdet, processer for behandling af data, styring af leverandører og tekniske sikkerhedsforanstaltninger.
Myndighederne	"Myndighederne" er i denne undersøgelse de 17 ministerier, som indgår i undersøgelsen, og Region Midtjylland.
Outsourcing	Outsourcing betyder, at en opgave, fx drift, vedligeholdelse og udvikling af it-tjenester, overlades til en ekstern leverandør. Det kan enten være en privat virksomhed eller en anden offentlig myndighed.
Persondataloven	Persondataloven er en tidligere dansk lov om behandling af personoplysninger, som implementerede databeskyttelsesdirektivet i dansk lov. Persondataloven var gældende fra 2000 og blev i 2018 erstattet af GDPR (databeskyttelsesforordningen) og databeskyttelsesloven.
Planlagte tilsyn	Planlagte tilsyn er tilsyn, som iværksættes på baggrund af Datatilsynets halvårlige tilsynsplaner.
Retshåndhævelsesloven	Retshåndhævelsesloven (lov nr. 410 af 27. april 2017) trådte i kraft den 27. april 2017. Retshåndhævelsesloven gælder for retshåndhævende myndigheders (politi, anklagemyndighed, Kriminalforsorgen, Den Uafhængige Politianklagemyndighed og domstolene) behandling af personoplysninger på det strafferetlige område og træder i stedet for GDPR og databeskyttelsesloven. Mange af kravene i retshåndhævelsesloven er imidlertid sammenfaldende med reglerne i GDPR, herunder reglerne om risikovurderinger, databehandleraftaler og tilsyn.
Specifik revisorerklæring	En specifik revisorerklæring omfatter det specifikke it-system eller den specifikke databehandling, som myndigheden har outsourcet.
Specifik godkendelse af underdatabehandlere	Myndighederne kan i databehandleraftalen indskrive et krav om en specifik godkendelse af underdatabehandlere. Det betyder, at databehandleren ikke må benytte en ny underdatabehandler, før myndigheden specifikt har godkendt den nye underdatabehandler.
Tredjelande	Tredjelande er lande, som ikke er medlem af EU eller EØS (Island, Lichtenstein og Norge). Som udgangspunkt er alle lande uden for EU/EØS at betragte som usikre tredjelande. Europa-Kommissionen har imidlertid afgjort, at beskyttelsesniveauet for en række tredjelande lever op til sikkerhedsstandarderne, der gælder inden for EU, og dermed kan betragtes som sikre tredjelande. Det gælder fx Schweiz, New Zealand og organisationer/virksomheder i USA, som har tilsluttet sig EU-U.S. Privacy Shield.