



## **Tilsyn med sagsbehandlende it-løsninger om den digitale forvaltnings hyldevarer**

Motzfeldt, Hanne Marie

*Published in:*  
Nordisk Administrativt Tidsskrift

*Publication date:*  
2016

*Document version*  
Også kaldet Forlagets PDF

*Citation for published version (APA):*  
Motzfeldt, H. M. (2016). Tilsyn med sagsbehandlende it-løsninger: om den digitale forvaltnings hyldevarer. *Nordisk Administrativt Tidsskrift*, 93(2), 17-33. <https://www.djoef-forlag.dk/sites/nat/index.php>

# Tilsyn med sagsbehandlende it-løsninger – om den digitale forvaltnings hyldevarer

*Af Hanne Marie Motzfeldt*

*Refereevurdert*

## 1. Indledning

I det følgende tages det op, om den almindelige, danske forvaltningsret stiller krav til myndighedernes viden om og indsigt i de på forhånd udviklede it-systemer, som myndighederne anskaffer til at håndtere borgernes sager.<sup>1</sup> Udgangspunktet er de almindelige principper om forvaltningsmyndigheders pligt til at føre tilsyn med eksterne leverandørers opgaveløsning – og formålet er at afklare betydningen af denne tilsynspligt, når myndighederne anskaffer præfabrikerede, sagsbehandlende it-løsninger og efterfølgende outsourcer drift og vedligehold.<sup>2</sup>

Spørgsmålet er af stigende betydning, idet danske forvaltningsmyndigheder i vidt omfang anskaffer informations- og kommunikationsteknologi til at løse deres opgaver. Mange af de systemer, myndighederne betaler for at anvende, er udviklet til flere eller mange myndigheder. Med andre ord er der tale om på forhånd udviklede standardløsninger. Udviklingen af disse systemer pågår primært i private virksomheder. Heller ikke efterfølgende drift og vedligehold varetages videre hyppigt af myndighederne selv. Opgaverne udliciteres (outsources), dvs. drift- og vedligeholdsopgaver overføres til de private virksomheder, der udbyder løsningerne.<sup>3</sup> Med andre ord udvikles, udbydes, drives og vedligeholdes disse standardløsninger af private leverandører.

Nutidige it-løsninger kan programmeres til at varetage sagsbehandlingsfunktioner i afgørelsessager. Systemerne kan eksempelvis starte sager op, vejlede borgerne og indhente de nødvendige oplysninger i de sager, der håndteres af løsningerne. Enkelte systemer kan også træffe afgørelse overfor borgerne, meddele eller ligefrem effektuere disse afgørelser. En række danske it-løsninger er således sagsbehandlende, samtidig med at de udvikles, drives, vedligeholdes og serviceres af private virksomheder.

Udbuddet af sådanne på forhånd udviklede systemer øges i disse år – det vil sige, at sagsbehandlende it-løsninger i et vist omfang udbydes som »hyldevarer« på det danske marked.

Allerede da den digitale forvaltning var i et meget tidligt udviklingsstadium, blev det i en større dansk redegørelse om mulighederne for at udlicitere myndighedsopgaver anført, at der burde etableres visse retssikkerhedsgarantier, når sagsbehandlende it-systemer udvikles, udbydes, drives og vedligeholdes af private leverandører. Et forslag til en sådan retssikkerhedsgaranti var, at myndigheder skulle have fuld adgang til og indsigt i de kontraherende virksomheders sagsbehandlingsprogrammer.<sup>4</sup>

Til trods for, at der i dag – som beskrevet – anvendes sagsbehandlende løsninger og at disse udvikles af private aktører, kan det konstateres, at danske myndigheder næppe har videre omfattende viden om eller indsigt i deres it-systemer. I 2015 blev der – i forlængelse af alvorlig kritik af systemet fra den danske ombudsmand i FOB 2014-24 – foretaget en undersøgelse af en fejlbehæftet, sagsbehandlende it-løsning inden for skatteområdet, EFI.<sup>5</sup> Under det politiske efterspil blev det afdækket, at de ansvarlige myndigheder manglede overblik over og indsigt i de over 200 it-systemer, der anvendes inden for skatteområdet. Den danske skatteminister erkendte, at:

*»[v]iden om, hvordan de data og forretningsprocesser, som er 'støbt' ned i it-systemerne, helt præcist hænger sammen, er dermed i høj grad placeret hos SKATs it-leverandører og ikke hos SKAT selv. Derudover er data og systemer i mange tilfælde dårligt dokumenterede, og SKAT har derfor ikke tilstrækkeligt indblik i dem. Disse strukturelle udfordringer begrænser SKATs muligheder for selv at styre og kontrollere udviklingen af it-understøttelsen. Det gør det også svært at konkurrenceudsætte systemerne, at skifte leverandør, og at skabe sikkerhed for, at løsningerne følger lovens krav og er fleksible, så de kan tilpasses, når regler eller behov ændres.«<sup>6</sup>*

Tilsvarende måtte Rigspolitiet i 2015 undlade at sende det danske politis it-systemer i udbud. Årsagen var, at systemerne var så ringe dokumenterede, at det blev vurderet, at det reelt ikke var muligt for andre end den hidtidige leverandør at byde på opgaven.<sup>7</sup>

Da fokus i den følgende undersøgelse af myndighedernes tilsynspligt er rettet mod på forhånd udviklede, sagsbehandlende it-løsninger, beskrives det indledningsvis kort i afsnit 2, hvad der i nærværende sammenhæng forstås ved sagsbehandlende it-systemer. Derefter vendes blikket mod principperne om forvaltningsmyndigheders pligt til tilsyn med eksterne leverandører. Efter en overordnet beskrivelse i afsnit 3.1. afgrænses i afsnit 3.2., hvilke forhold der skal føres tilsyn med. I afsnit 3.3. ses der nærmere på omfanget og indholdet af pligten til tilsyn med sagsbehandlende it-løsninger. Idet det vurderes, at tilsynspligten er skærpet, når myndigheder løser deres opgaver ved brug af sagsbehandlende it-løsninger, opdeles derefter af hensyn til overskueligheden i afsnit 3.3.1. og 3.3.2. I disse afsnit undersøges først betydningen af de ulovbestemte principper i forbindelse med anskaffelse og ibrugtagelse af systemerne. Derefter undersøges kravene ved myndighedernes brug af og virksomhedernes drift af de sagsbehandlende løsninger i afsnit 3.3.2. I afsnit 4 afsluttes med opsummering og konklusion.

## 2. Sagsbehandlende it-løsninger

Det er langt fra alle former for informations- og kommunikationsteknologi, der kan overtage egentlige sagsbehandlingsfunktioner fra menneskelige sagsbehandlere i afgørelsessager. Nogle systemer udfører kun relativt enkle opgaver efter at blive aktiveret af en kommando fra en offentlig ansat. Det er for eksempel tekstbehandlingssystemer eller journalssystemer. Andre systemer er derimod programmeret til automatisk at foretage visse sagsbehandlingsskridt, når bestemte forudsætninger er opfyldt – vel at mærke uden intervention fra en fysisk person.<sup>8</sup>

I dag kan sagsbehandlende systemer ofte indgå i direkte interaktion med borgerne, eksempelvis modtage ansøgninger og indberetninger via selvbetjeningsløsninger. Derudover kan sådanne systemer typisk indhente (yderligere) information fra offentlige databaser mv., og på den baggrund foretage kontroller, udføre beregninger, generere skrivelser eller foretage handlinger. Sådanne handlinger kan for eksempel være forelæggelse for sagens parter eller underretning af andre myndigheder. Som det er nævnt indledningsvis, kan enkelte systemer også selv meddele afgørelser til borgerne eller endda effektuere disse. I andre tilfælde anvendes, justeres, tilpasses og kontrolleres det automatiske genererede materiale af en menneskelig sagsbehandler.

Brug af sagsbehandlende it-systemer indebærer, at større eller mindre dele af den retlige beslutningsproces overtages af systemet i den enkelte afgørelsessag. Dette omfatter anvendelse af både formelle og materielle regler (sagsbehandlingsregler og indholdsmæssige krav). Sådant prædefineret og automatiseret sagsbehandling indebærer, at borgerens retsstilling i den konkrete afgørelsessag i realiteten helt eller delvist bliver fastlagt på forhånd via systemets programmering. Fejl eller mangler i programmeringen af de sagsbehandlende it-løsninger kan dermed påvirke borgernes retsstilling betydeligt.

Sagsbehandlende it-løsninger kan blive specielt udviklet til en enkelt myndighed, som for eksempel det ovenfor nævnte EFI-system. Løsningerne kan også være de her omhandlede præfabrikerede ”hyldevarer”, som mange myndigheder kan bruge. Sådanne præfabrikerede systemer kan blandt andet findes i kataloger fra en af de store leverandører af digitale løsninger på det danske marked, KMD A/S.

Et eksempel er KMD Boliglån ASP, der understøtter myndighedernes behandling af borgernes ansøgninger om samt administration og opkrævning af beboerindskudslån inden for det sociale område. Ved oprettelse af en låneansøgning henter systemet automatisk relevante oplysninger om beboere og bolig samt validerer disse informationer via blandt andet de danske valglisten. Systemet beregner borgerens lån og håndterer fastlæggelse af afviklingstid, månedlige ydelser samt efterfølgende låneafvikling. Løsningen sikrer desuden automatisk advis ved ophør af afdragsfrihed, fraflytning eller dødsfald, ligesom systemet genererer en årlig datafil til de danske skattemyndigheder til brug for ligning af borgerens skat.

Der kan være praktiske, tekniske eller økonomiske forhold, der begrunder, at allerede færdigudviklede it-løsninger vanskeligt kan ændres og tilpasses en enkelt myndigheds behov eller til ændrede omstændigheder. Det er imidlertid en fast og accepteret bestanddel af dansk ombudsmandspraksis, at de forvaltningsretlige regler og principper gælder, uanset om »leverandørerne af IT-løsninger slet ikke udbyder en løsning, som kan opfylde kravene«.<sup>9</sup> Argumentationen er – kort fortalt – at de teknologineutrale, danske forvaltningsretlige regler skal overholdes, uanset valg af arbejdsredska-

ber. Er ikke andet bestemt i loven, må myndighederne håndtere sagerne manuelt, hvis brug af digitale løsninger fører til administration i strid med loven. Med andre ord er det fra en dansk forvaltningsretlig vinkel principielt uden betydning, om en given teknologi er en præfabrikeret ”hyldevare” eller ej. Heraf følger, at de præfabrikerede, sagsbehandlende løsninger skal leve op til de forvaltningsretlige krav på samme vis som løsninger udviklet specielt til en enkelt myndighed.

### 3. Pligten til at føre tilsyn med outsourcete, sagsbehandlende it-løsninger

Der er ikke megen dansk rets-, ombudsmands- eller administrativ praksis om myndigheders ulovbestemte forvaltningsretlige pligt til at føre tilsyn med de it-systemer, der leveres og drives af private it-leverandører. Som det er nævnt ovenfor, er de almindelige forvaltningsretlige regler imidlertid teknologineutrale. Formodningen er dermed for anvendelse af de samme principper, som gælder for tilsyn med private leverandører af andre varer og ydelser i den manuelle forvaltning. Disse principper er derfor det naturlige udgangspunkt i det følgende.

#### 3.1. Overordnet om tilsynspligten

Det antages i dansk litteratur og praksis, at forvaltningsmyndigheder på ulovbestemt grundlag har pligt til at føre tilsyn med udførslen af de myndighedsopgaver, der udliciteres til private. Det bagvedliggende synspunkt er, at tilsynspligten er en naturlig følge af, at myndigheden forsat bærer ansvaret for opgavens udførelse.<sup>10</sup> Tilsvarende er lagt til grund i dansk lovgivningspraksis. Det fremgår eksempelvis af forarbejderne til den danske regionslov, at regionsrådene ikke kan frasige sig ansvaret for opfyldelse af lovgivningens krav til opgavevaretagelse ved at indgå aftaler med private leverandører.<sup>11</sup>

En af de mere uddybende udtalelser fra den danske ombudsmand om tilsynspligt i den manuelle forvaltning er FOB 2010 20-14.<sup>12</sup> Baggrunden for sagen var et samarbejde mellem flere kommuner, hvorefter en række private virksomheder leverede ydelser til borgerne. Blandt de ydelser der blev leveret af de private virksomheder, var ortopædisk skotøj, som borgerne havde fået bevilget efter den sociale lovgivning. En borger var utilfreds med de skoindlæg, han havde fået tilvirket hos en af leverandørerne og klagede til kommunen. Da både kommunen og klagemyndighederne afviste borgerens henvendelse, endte sagen hos Folketingets Ombudsmand – og mandede ud i en redegørelse for kommunens tilsyns- og reaktionspligt i forhold til den private leverandør.

Om pligten til tilsyn udtalte embedet generelt:

*»Det gælder således at når en myndighed indgår aftale med en virksomhed om at virksomheden mod betaling skal levere ydelser til myndigheden eller til borgerne, så skal myndigheden føre tilsyn med at virksomheden opfylder de krav som fremgår af aftalen og de relevante bestemmelser i lovgivningen. Tilsynet skal føres så længe aftalen løber.«*

Det er naturligt at antage, at denne tilsynspligt også er gældende, når der anskaffes og ibrugtages præfabrikerede, sagsbehandlende it-løsninger og driften af disse udliciteres (outsources). Også i den digitale forvaltning er det en væsentlig pointe, at »det er

den enkelte myndigheds ansvar, at dens løsninger lever op til de forvaltningsretlige krav«. <sup>13</sup> Hensynet til fastholdelse af dette ansvar hos myndigheden gør sig således gældende i den digitale forvaltning – og begrundet pligten til tilsyn på tilsvarende vis som i den manuelle forvaltning. Dertil kommer, at hensynet til at sikre en økonomisk forsvarlig forvaltning taler for et vist tilsyn med aftalens overholdelse – et hensyn, der også nævnes af den danske ombudsmand i FOB 2010 20-14.

Anvendelse af den almindelige forvaltningsretlige tilsynspligt i forhold til den informations- og kommunikationsteknologi, der leveres af eksterne leverandører til den digitale forvaltning, indebærer, at danske forvaltningsmyndigheder blandt andet skal føre tilsyn med de it-leverandører, der leverer sagsbehandlende løsninger til myndighederne. Følges linjen i FOB 2010 20-14 gælder denne pligt, uanset om systemet indgår i direkte interaktion med borgerne eller ej. Det er således uden betydning for selve eksistensen af forpligtelsen, om systemet blot bistår myndighedens ansatte med kontroller, beregninger, udkast til skrivelser og lignende, eller om det indeholder selvbetjenings- og sagsafgørende elementer.

Det kan konkluderes, at de ulovbestemte principper om tilsynspligt også finder anvendelse, når forvaltningsmyndigheder anskaffer og anvender sagsbehandlende it-løsninger, der udbydes, drives og vedligeholdes af private virksomheder.

### 3.2. Afgrænsning af tilsynstemaet

En forvaltningsmyndigheds aftale med en privat virksomhed om leverance af et it-system samt drift og vedligeholdelse heraf kan næppe antages at forpligte eller berettige den aftaleindgående myndighed til at føre tilsyn med (alle) virksomhedens forhold. I den ovenfor omtalte udtalelse fra den danske ombudsmand om opgaver udført af en ekstern leverandør af ortopædiske sko, udtalte embedet:

*»Det handler her om at sikre, at den faglige kvalitet og omkostningerne nøje svarer til, hvad kommunalbestyrelsen eller amtsrådet ønsker og vil tage ansvar for.«*

Tilsvarende synes dansk lovgivningspraksis ved fastsættelse af særbestemmelser om tilsyn med private leverandører at fokusere på de kvalitetsstandarder, som den aftaleindgående myndighed har fastsat inden for lovgivningens rammer. Et eksempel er retssikkerhedslovens § 16 om myndighederne pligt til at foretage aktivt tilsyn med de opgaver, der løses af private leverandører på det sociale område. <sup>14</sup> Det fremgår af forarbejderne til bestemmelsen, at formålet er at sikre, at opgaverne løses med den kvalitet – både fagligt og økonomisk – som myndigheden inden for lovgivningens rammer har besluttet, der skal være. <sup>15</sup> Dette dobbelte fokus på overholdelse af relevant lovgivning henholdsvis opfyldelse af aftalte standarder synes da også at stemme med koblingen mellem aftaleindgåelse, specifikation af ydelsen og tilrettelæggelse af tilsyn i FOB 2010 20-14:

*»Når det drejer sig om, at andre udfører en opgave for det offentlige, er det vigtigt, at myndigheden allerede, når aftalen indgås, stiller krav om, at aftalens økonomiske dele suppleres med beskrivelser af kvaliteten af den ydelse, som skal leveres. Uden en sådan beskrivelse er det ikke forsvarligt at indgå aftale om udførelse af en opgave.*

*Det bør også af aftalen fremgå, hvordan der i forbindelse med den løbende drift skal ske kontrol af, at opgaven udføres med den aftalte og ønskede kvalitet. Der vil fx blive vejledt om, hvordan krav om kvalitet og kontrol hermed kan indgå i aftalerne, hvordan det sikres, at forvaltningslovens regler kan efterleves, statistik-produktion, m.v.«*

Med andre ord må den ulovbestemte tilsynspligt naturligt rette sig mod forhold, der er relateret til de opgaver, der overlades til den private leverandør. Danske forvaltningsmyndigheder er i almindelighed forpligtet til at sikre, at deres it-systemer er designet på en sådan måde, at både almindelige og specielle regler overholdes, når systemerne anvendes.<sup>16</sup> Tilsynets formål er dermed sikring af, at systemet er programmeret og kontinuerligt indstillet til at sikre overholdelse af relevant lovgivning, når it-løsningen håndterer borgernes sager og at ydelsen i øvrigt svarer til de kvalitetsstandarder og andre udfyldninger, som myndigheden har fastsat inden for lovgivningens rammer.<sup>17</sup> Sidstnævnte kan eksempelvis vedrøre driftssikkerhed eller brugervenlighed.

Opsummerende er der – i relation til sagsbehandlende it-systemer – to centrale tilsynstemaer. Det ene tema er, at systemet er designet og indstillinger sat til at sikre overholdelse af den relevante lovgivning i de sager, systemet håndterer. Det andet tema er opfyldelse af de kvalitetsstandarder, som myndigheden har fastsat på it-området.

### 3.3. Omfang og indhold af tilsynspligten

Til trods for enighed om en vis skærpelse af tilsynspligten, når der sker overladelse af opgaver til private, anser litteraturen ikke denne ulovbestemte pligt som værende særlig vidtgående.<sup>18</sup> Der er – så vidt vides – ikke nærmere beskrivelser af indhold og omfang af forpligtelsen i litteraturen. I FOB 2010 20-14 om de potentielt mangelfulde skøindlæg sammenlignes pligten til tilsyn med opgaver udført af eksterne leverandører med det tilsyn, der skal føres i forbindelse med forvaltningens egen, interne opgaveløsning.<sup>19</sup>

Jens Peter Christensen er den danske forfatter, der mest indgående har beskæftiget sig med den interne tilsynspligt – forstået som overordnede embedsmænds ansvar for tilsyn med deres administrationsområder. I en fremstilling fra 2002 tager forfatteren udgangspunkt i den regel, der er udtrykt i den danske ministeransvarslovs bestemmelse om medvirken.<sup>20</sup> En minister anses som ansvarlig for en underordnetes handling efter denne bestemmelse, når ministeren har fremmet handlingens udførelse ved ikke i ”rimeligt” omfang at føre tilsyn og fastsætte instrukser.<sup>21</sup> Efter en gennemgang af flere konkrete sager, konkluderer Jens Peter Christensen imidlertid, at det ”nærmere indhold og omfang af topchefers tilsynspligt må – i mangel af mere præcise bestemmelser eller praksis – søges fastlagt ud fra friere retlige overvejelser.” En nyere beretning fra en dansk kommissionsundersøgelse synes at bekræfte, at forfatterens beskrivelse stadig er dækkende for retsstillingen i Danmark:

*»En overordnet embedsmand har pligt til at holde sig orienteret inden for sit område og til at føre et vist tilsyn med, hvad der foregår. Endvidere må den overordnede i formødent omfang fastsætte instrukser for behandlingen af sager mv. inden for sit sagsområde.*

*Topchefer er i almindelighed berettiget til at gå ud fra, at sager, der varetages af underordnede, varetages lovligt og korrekt, således at topchefens ansvar indskrænker sig til et ansvar for, at opgaven varetages af formodningsvis kyndige.«<sup>22</sup>*

Lægges sammenligningen med det interne tilsyn i FOB 2010 20-14 uden videre til grund, synes pligten til tilsyn i forbindelse med anskaffelse, ibrugtagelse og anvendelse af de her omhandlede it-løsninger således ikke umiddelbart at indebære særlig vidtgående pligter for forvaltningsmyndighederne. Heroverfor står imidlertid, at der bør udvises en vis forsigtighed med unuanceret og mekanisk at overføre de alminde-

lige forvaltningsretlige principper og retsgrundsætninger fra den manuelle forvaltning på forholdene i den digitale forvaltning. Nye arbejdsgange- og konstruktioner samt arbejdsredskaber i den digitale forvaltning bør håndteres i lyset af deres karakteristika og ud fra formålet og grundtankerne med de almindelige forvaltningsretlige principper. Det nærmere indhold af den forvaltningsretlige tilsynspligt i forbindelse med anskaffelse og anvendelse af private virksomheders præfabrikerede, sagsbehandlende it-løsninger må derfor – som antaget af Jens Peter Christensen – bero på friere retlige overvejelser.

Her kan blikket først og fremmest rettes mod de hensyn, der kan begrunde tilbageholdenhed i forhold til i det hele taget at overlade opgaven med at udvikle og drive sagsbehandlende it-løsninger til private virksomheder. Helt centralt er, at samarbejde med private virksomheder kan være problematisk som følge af, at private aktører ikke bindes af de forvaltningsretlige regler. Det betyder blandt andet, at det er forvaltningsmyndighederne, ikke virksomhederne, der er omfattet af principperne om at indbygge de forvaltningsretlige regler i it-løsninger.<sup>23</sup> Også hensynet til åbenhed er relevant, idet det ikke er givet, at borgerne får adgang til informationer om den programmering, der ligger bag sagsbehandlende it-løsningers opbygning og funktionaliteter samt indbyggede sagsgange. Dertil kommer, at kompetence til at fortolke og udfylde både almindelige forvaltningsretlige regler og relevant speciallovgivning er essentiel, når disse skal indbygges i de sagsbehandlende it-systemer. En myndighed kan i almindelighed ikke – som en topchef i det offentlige i forhold til sine ansatte – gå ud fra, at en privat virksomhed med en teknisk-faglig profil har de fornødne kompetencer til at fortolke og udfylde lovgivningen.

I forlængelse af sidstnævnte kan det drøftes, om sammenligningen mellem pligten til tilsyn med opgaver udført af private leverandører og det interne tilsyn i det hele taget er rammende. Den umiddelbare lighed består i, at begge tilsynspligter bygger på hensynet til at fastholde ansvaret for opgavernes tilrettelæggelse og udførelse hos den oprindeligt ansvarlige (myndigheden henholdsvis den overordnede). Intern (uegentlig) delegation finder imidlertid sted i et andet retligt miljø, end når opgaver overlades til private virksomheder. En offentlig leder har grund til at forvente, at underordnede handler inden for lovgivningens og forvaltningsrettens rammer, når borgernes sager behandles – og underretter ledelsen, hvis dette ikke er muligt.<sup>24</sup> Offentlig ansatte er forpligtet til at udføre deres opgaver lovligt og forsvarligt efter den danske tjenestemandsløvs § 10 og princippet i bestemmelsen.<sup>25</sup> Samtidig er det ansvarspådragende for offentlig ansatte, hvis lovpligtige opgaver ikke udføres, jf. eksempelvis UfR 2009.999 H, ligesom forsømmelse og skødesløshed generelt er sanktioneret i den danske straffeløvs §§ 155, 156 og 157.<sup>26</sup> Der er ikke en tilsvarende regulering af private virksomheders pligter, når de udfører opgaver for forvaltningsmyndigheder. Uagtet at enkelte forhold for private leverandører også er reguleret i straffeloven, som f.eks. tavshedspligt, kan de øvrige dele af dette retlige miljø næppe fuldt ud overføres til den private sektor via kontraktsregulering. Derfor kan myndighederne ikke med rette have samme høje forventninger til private leverandører, som de kan have til egne ansatte.

Dertil kommer, at det i litteraturen blandt andet fremhæves som en betænkelighed ved at overlade opgaver til private virksomheder, at det kan være vanskeligt at kontrollere og tilbagekalde en given delegation.<sup>27</sup> Som en mere retspolitisk betragtning er det desuden blevet anført, at profitorienteringen i den private sektor kan indebære



en vis risiko for ringere kvalitet af ydelser sammenlignet med løsning af opgaver i den offentlige sektor.<sup>28</sup>

Der er med andre ord en række hensyn, der i dansk litteratur og praksis hidtil har begrundet den opfattelse, at kun udførelse af faktisk forvaltningsvirksomhed kan overlades til private uden lovhjemmel.<sup>29</sup> Overladelser af myndighedsopgaver forudsætter derimod klar hjemmel i lov. Dette er relevant i nærværende sammenhæng, fordi der må antages at være et vist samspil og harmoni mellem de almindelige, ulovbestemte principper i den danske forvaltningsret; her læren om delegation uden lovhjemmel og principperne om tilsynspligt. Den her omhandlede, ulovbestemte tilsynspligt må i sagens natur være udviklet til primært at håndtere den situation, der opstår i forlængelse af en ulovbestemt delegation – ikke en delegation bestemt i en særskilt lovbestemmelse, hvor der ved udformningen af lovgivningen er anledning til at tage stilling til tilsynsaspektet.<sup>30</sup>

Da den parallelle lære om ulovbestemt delegation normalt afskærer myndighederne fra delegation af myndighedsudøvelse til private virksomheder, er den ulovbestemte tilsynspligt udviklet til at håndtere udlicitering af faktisk forvaltningsvirksomhed, som f.eks. tilvirkning af sko eller kørsel med ambulancer. Dermed hviler opfattelsen af, at myndigheder ikke har en særlig vidtgående pligt til at føre tilsyn med opgaver udført af private leverandører på en forudsætning om, at den private virksomhed kun udfører opgaver, der har karakter af faktisk forvaltningsvirksomhed. Den hidtidige praksis har derimod ikke forholdt sig til tilsyn med sagsbehandlende it-løsninger, hvis programmering kan få betydelig indflydelse på indholdet af de afgørelser, der træffes i forhold til borgerne.

Anskaffelse og ibrugtagelse af præfabrikerede, sagsbehandlende it-løsninger samt outsourcing af drift til private virksomheder udgør således en hybrid i denne sammenhæng. De sagsbehandlende it-løsninger skiller sig ud, idet de skal behandle og i visse tilfælde træffe afgørelse i borgernes konkrete sager. Som det er beskrevet i afsnit 2, kan den programmering, der styrer den automatiske sagsbehandling i disse systemer få betydelig indflydelse på borgernes processuelle og materielle retsstilling. En aftale om adgang til, ibrugtagning af samt efterfølgende drift af et it-system, der behandler og eventuelt træffer afgørelse i borgernes sager, adskiller sig således væsentligt fra tilvirkningen af de potentielt mangelfulde skoindlæg i FOB 2010 20-14.

Om end programmeringen næppe har den samme betydning for borgerens retsstilling i alle tilfælde, synes forbindelsen mellem forudgående programmering og senere fastlæggelse af borgerens retsstilling i de konkrete sager, der håndteres af et sagsbehandlende it-system, at være et hensyn der begrundet en skærpelse af tilsynspligten. Forvaltningsmyndighedernes tilsyn med sagsbehandlende it-løsninger bør således være mere intensivt end i forhold til andre former for ydelser, der leveres af private virksomheder til myndigheder eller borgere.

Det synes oplagt, at en sådan skærpet tilsynspligt forudsætter, at danske forvaltningsmyndigheder har en vis viden om, indblik i og dokumentation af de sagsbehandlende it-løsninger, myndighederne anvender til at håndtere borgernes sager. Af hensyn til overskueligheden ses i det følgende først på tilsyn i forbindelse med myndighedernes anskaffelse og ibrugtagning i afsnit 3.3.1., derefter på den efterfølgende anvendelse og drift i afsnit 3.3.2.

### 3.3.1. nskaffelse og ibrugtagning

Til trods for det i afsnit 3.2. anførte, kan det have sine fordele indledningsvis at sammenholde med den interne tilsynspligt, når det skal vurderes, om og i hvilket omfang forvaltningsmyndigheder har pligt til at sikre sig viden om, hvordan et it-system er programmeret til at håndtere borgernes sager, inden systemet anskaffes og tages i brug.

Manglende viden om den programmering og de funktionaliteter, der styrer håndteringen af borgernes sager, vil svare til, at en overordnet leder ikke holder sig orienteret om, hvordan et ansvarsområde administreres – eller ligefrem overlader fastsættelse af retningslinjer for behandling af borgernes sager til en privat virksomhed. Derudover er viden om programmering og funktionaliteter en forudsætning for at fastholde myndighedens ansvar for systemets efterlevelse af lovgivningen og eventuelle aftalte standarder. Reale hensyn – friere retlige overvejelser – synes således at lede til, at en dansk forvaltningsmyndighed ikke kan tage en på forhånd udviklet og sagsbehandlende it-løsning i brug uden en vis forudgående indsigt i programmet.

Dette synes da også at harmonere med den danske ombudsmands holdning i EFI-sagen, om end sagen ikke drejede sig om de præfabrikerede hyldevarer, der er i fokus i nærværende sammenhæng. I den tidligere nævnte udtalelse om EFI, FOB 2014-24, udtalte Folketingets ombudsmand kritik af, at systemet var blevet sat i drift, inden det var tilstrækkeligt undersøgt, om løsningen overholdt de forvaltningsretlige krav.<sup>31</sup> Ombudsmanden uddybede:

*»Efter min opfattelse er det således ikke tilfredsstillende, at en dækkende beskrivelse af, hvorledes de forvaltningsretlige krav vil blive overholdt i IT-systemet, først blev tilvejebragt efter, at systemet delvist var sat i drift. Det er et grundlæggende krav, at IT-systemer kan understøtte en korrekt anvendelse af relevant lovgivning ...«*

Spørgsmålet er herefter, hvad der nærmere ligger i en dækkende beskrivelse – dvs. hvilke krav der stilles til forvaltningsmyndighedernes viden om de it-løsninger, myndighederne påtænker at anvende. I den forbindelse kan det være relevant at overveje betydningen af, at myndighedernes brug af sagsbehandlende it-løsninger stort set altid vil indebære, at der sker elektronisk behandling af personoplysninger.

I første omgang indebærer den omstændighed, at der håndteres personoplysninger i en outsourcet it-løsning, at den private virksomhed regnes som databehandler efter den danske persondatalovs § 3, nr. 5.<sup>32</sup> Det er dog stadig den dataansvarlige myndighed, der har ansvaret for, at behandlingen af personoplysninger i systemet er tilrettelagt på en måde, som sikrer overholdelse af persondatalovens og sikkerhedsbekendtgørelsens regler.<sup>33</sup> Myndigheden skal derfor sikre overholdelse, inden behandling påbegyndes og instruere den databehandlende leverandør heri. Myndigheden skal i den forbindelse indgå en databehandleraftale med leverandøren, og det fremgår af det danske Datatilsyns retningslinjer, at detaljeringsgraden af aftale samt instrukser skal modsvare systemets kompleksitet.<sup>34</sup> Derudover stiller Datatilsynet i praksis en række mere konkrete krav til de dataansvarliges viden om den behandling af personoplysninger, som deres databehandlere skal udføre. Et eksempel er, at en dataansvarlig myndighed skal vide, hvor oplysninger fysisk befinder sig (dvs. på hvilke servere).<sup>35</sup> Et andet eksempel er, at myndigheden skal sikre overholdelse af kravet om logning i sikkerhedsbekendtgørelsens § 19.<sup>36</sup> Tilsynets krav retter sig dog ikke alene mod indhold og omfang af de dataansvarliges viden om behandlingerne hos databehandlerne, men også mod troværdigheden af den information, som myndigheden modta-

ger fra databehandleren. Datatilsynet stiller således i visse tilfælde krav om, at en databehandlers information om behandling af personoplysninger skal være valideret.<sup>37</sup> Sidstnævnte kan være i form af en it-revisionsrapport udarbejdet af en uvildig tredjemand.<sup>38</sup>

Fra den 25. maj 2018 vil det desuden være et udtrykkeligt krav, at en dataansvarlig myndighed til enhver tid kan påvise, at behandlingen af oplysninger i et sagsbehandlingssystem overholder de persondatarelige regler, jf. persondataforordningens artikel 24, stk. 1.<sup>39</sup> I forlængelse heraf stilles krav om, at der bliver ført en ganske detaljeret skriftlig fortegnelse over alle behandlinger, jf. artikel 30, stk. 1, samt præambelens betragtning 82.<sup>40</sup> Overholdelse af de kommende persondatarelige regler forudsætter med andre ord, at myndigheden har adgang til omfattende og validerbare informationer om it-systemet, der gør det muligt at påvise compliance.

En følge af den persondatarelige regulering af forholdet mellem databehandler og dataansvarlig er således, at en dataansvarlig myndighed skal have indsigt i og (troværdig) dokumentation for den behandling af personoplysninger, der påtænkes fortaget i præfabrikerede, sagsbehandlingssystemer. Informationerne om systemet skal tilvejebringes, inden der behandles personoplysninger i systemerne, idet behandlingen ellers ikke må iværksættes.

Det er ikke urealistisk, at den veludviklede regulering af forholdet mellem dataansvarlig myndighed og databehandlende it-leverandør kan få en afsnittende virkning på de forvaltningsretlige krav til myndigheders indsigt i sagsbehandlingssystemer. Der er eksempler på, at de persondatarelige regler tidligere har haft betydning for udviklingen af den danske forvaltningsret. Det bedste eksempel er en ombudsmandssag, FOB 2005.309, om offentliggørelse af oplysninger om en virksomhed.<sup>41</sup> Selvom den danske persondatalovs regler kun regulerer behandling af oplysninger om fysiske personer, udtalte den danske ombudsmand alligevel i sagen, at de generelle principper i persondatalovens § 5 også gælder for behandling af oplysninger om virksomheder.

Baggrunden for sagen var en klage fra et luftfartsselskab til Folketingets Ombudsmand. Selskabet klagede over, at Forbrugerombudsmanden via Forbrugerstyrelsens hjemmeside havde offentliggjort en beslutning i en sag. Selskabet navn var angivet i det offentliggjorte materiale. Det fremgik desuden, at Forbrugerombudsmanden havde meldt selskabet til politiet. Folketingets ombudsmand fastslog, at reglerne om tavshedspligt ikke var til hinder for offentliggørelsen. Herefter tilføjede ombudsmanden imidlertid, at det følger af det almindelige forvaltningsretlige saglighedsprincip, at en myndighed ikke uden hjemmel i lovgivningen eller (anden) saglig grund må offentliggøre oplysninger om en virksomhed, som må regnes som belastende for virksomheden. I den forbindelse henviste ombudsmanden til principperne i persondatalovens § 5. Om brugen af de grundlæggende persondatarelige principper i persondatalovens § 5, anføres i udtalelsen, at: »Da den foreliggende sag angår oplysninger om en virksomhed, finder persondataloven ikke anvendelse; men principperne i lovens § 5 er efter min mening af en så almen karakter at de i et vist omfang også finder anvendelse uden for persondatalovens anvendelsesområde.«

Det er ikke urealistisk, at den danske ombudsmand kan og vil anvende en kombination af persondatarelige tankegange og god forvaltningsskik til at udvikle forvaltningsretlige krav til validerbar dokumentation af sagsbehandlingssystemer, der svarer til de persondatarelige krav. Alt andet lige synes en risiko for krænkelse af retten til beskyttelse af personoplysninger ikke at være væsentlig mere indgribende i

forhold til borgerne end risikoen for ukorrekt sagsoplysning eller manglende iagttagelse af borgernes ret til vejledning, partsrepræsentation, partshøring, korrekt begrundelse, aktindsigt mv.

Der er dog for nuværende kun holdepunkter for at konkludere, at den forvaltningsretlige tilsynspligt i forhold it-leverandørers opgaveløsning indebærer, at myndighederne skal sikre sig en vis forudgående indsigt i en præfabrikeret, sagsbehandlende it-løsnings programmering og indbyggede funktionaliteter. Det er dog ikke urealistisk, at der med afsæt i god forvaltningsskik vil blive udviklet mere detaljerede og konkrete krav, eksempelvis om validerbar eller endda valideret dokumentation af systemerne.

### 3.3.2. Brug og drift

Til trods for, at tilsynspligten må regnes som skærpet i den her omhandlede kontekst, er der ikke umiddelbart mange holdepunkter for at stille krav om løbende tilsyn med it-leverandører under normal og uproblematisk drift af en sagsbehandlende it-løsning. I den flere steder omtalte FOB 2010 20-14, fastslog den danske ombudsmand da også, at myndigheder i den manuelle forvaltning har et betydeligt skøn ved tilrettelæggelsen af tilsyn med de opgaver, der udføres af eksterne leverandører. Med andre ord stillede embedet ikke krav om, at kommunen løbende og af egen drift foretog undersøgelser af, om leverancerne af skoindlæg levede op til lovgivningen og de aftalte kvalitetsstandarder.

Også her kan det imidlertid overvejes, hvilken betydning det har, at de sagsbehandlende it-løsninger indeholder elementer af myndighedsudøvelse, samtidig med at systemerne håndterer personoplysninger. Som dataansvarlig skal en myndighed ikke alene sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, men også *aktivt* påse, at sikkerhedskravene overholdes, jf. lovens § 42, stk. 1, og sikkerhedsvejledningens tekst til sikkerhedsbekendtgørelsens § 7.<sup>42</sup> Et tilsvarende krav vil gælde efter databeskyttelsesforordningen, som desuden vil stille krav om en egentlig procedure for regelmæssig efterprøvning af datasikkerhed i de her omhandlede it-løsninger, jf. forordningens artikel 33, stk. 1, litra d.

Det er fristende at udfylde de vage og ubestemte retsgrundsætninger i den almene forvaltningsret med persondatarettens i sammenligningen noget mere proaktive tilgang. Der er imidlertid ikke holdepunkter for en sådan udfyldning. Ud fra samme betragtninger som anført i afsnit 3.3.1. er det dog nærliggende at antage, at der på sigt og som led i god forvaltningsskik bliver udviklet lignende krav som led i tilsynet med overholdelse af de forvaltningsretlige krav til sagsbehandlende it-løsninger.

Manglende holdepunkter for, at der under normal og uændret drift gælder et dansk, forvaltningsretligt krav om løbende, aktivt tilsyn med overholdelse af de forvaltningsretlige krav til sagsbehandlende it-løsninger, er én ting. Forholdet er derimod et andet, hvis en myndighed modtager oplysninger, der giver rimelig grund til at antage, at borgernes sager ikke håndteres korrekt i systemet.

Som det blev omtalt i afsnit 3.2., udtalte den danske ombudsmand sig både om tilsynspligten og om reaktionspligten i FOB 2010 20-14 vedrørende den private leverandør af skoindlæg. Ombudsmanden fastslog, at kommunen i et vist omfang havde pligt til at reagere på – og nærmere undersøge rigtigheden af – oplysningerne fra borgeren om aftalebrud og manglende overholdelse af relevante bestemmelser i lovgivningen. I det konkrete tilfælde mente ombudsmanden, at borgerens henvendel-

se, pegede i retning af, at de kommunale opgaver ikke længere blev løst lovligt og rigtigt. Kommunen fik derfor kritik for ikke at have undersøgt nærmere, om borgernes oplysninger var korrekte.

Tilsvarende synes at være lagt til grund i FOB 2011 20-6. Sagen drejede sig om en kvinde, der var utilfreds med en privat leverandør af en ambulancetjenestes udrykningstid. I udtalelsen tog ombudsmanden udgangspunkt i, at det er regionerne, der bærer ansvaret for tilrettelæggelse af ambulanceberedskabet, og at regionerne derfor også skal føre tilsyn med, at indsatsen fungerer forsvarligt og efter hensigten. Derefter udtalte den danske ombudsmand:

»Når regionen som ansvarlig for tilrettelæggelsen af *den præhospitale indsats – efter en alvorlig hændelse – modtager en klage over en ambulances responstid, må regionen efter min opfattelse undersøge sagen forsvarligt for at finde ud af hvad der er sket.*

*Formålet med at undersøge sagen er for det første at regionen, som ansvarlig for den præhospitale indsats, kan tage stilling til om hændelsesforløbet giver regionen anledning til at reagere. For det andet vil en sådan undersøgelse danne grundlag for det svar som regionen skal give klageren.«*

Det kan således lægges til grund, at der i den manuelle forvaltning eksisterer en pligt til at reagere på oplysninger, der med en vis sandsynlighed indikerer, at eksterne leverandører ikke udfører deres opgaver i overensstemmelse med indgåede aftaler og lovgivningen.<sup>43</sup> Denne reaktionspligt afledes af tilsynspligten og indebærer, at myndigheden skal undersøge forholdene nærmere. For anvendelse af en lignende reaktionspligt i den digitale forvaltning taler, som tidligere anført, især hensynet til at fastholde ansvaret for opgavens udførelse og overholdelse af lovgivningen hos den myndighed, der anvender systemet.

Heraf kan udledes, at en dansk myndighed, som modtager oplysninger, der indikerer, at der er fejl og mangler ved en konkret, sagsbehandlende it-løsning, har pligt til at reagere på oplysningerne og undersøge forholdet. En forsvarlig undersøgelse må nødvendigvis kræve både viden om, indsigt i og tilvejebringelse af dokumentation for det konkrete system med henblik på at vurdere, om borgernes sager behandles lovligt og rigtigt i systemet.

Konstateres der ved en sådan nærmere undersøgelse fejl og mangler ved en it-løsning, skal det vurderes om manglerne fører til, at borgernes sager håndteres i strid med relevant lovgivning. Er dette tilfældet, peger dansk administrativ praksis i retning af, at myndighederne har en yderligere handlepligt; nemlig at rette op på de konstaterede mangler.<sup>44</sup>

Blandt andet på baggrund af udtalelsen i FOB 2014-9 om det sagsbehandlende it-system, EFI, bad SKAT i sommeren 2015 Kammeradvokaten om at gennemføre en såkaldt legalitetsanalyse af dele af systemet.<sup>45</sup> Analysen afdækkede en række fejl af varierende grovhed i systemet. Som opfølgning på undersøgelsen bad SKAT Kammeradvokaten om yderligere at vurdere, om dette førte til, at SKAT var helt eller delvis forpligtet til at indstille anvendelsen af systemet.<sup>46</sup> Kammeradvokaten skrev bl.a., når myndigheden:

»... er bekendt med eller har konkret og underbygget mistanke om, at anvendelse af et IT-system direkte eller indirekte fører til, at myndigheden handler ulovligt over for borgerne, må myndigheden enten undlade at anvende systemet eller sørge for, at eventuelle fejl afhjælpes manuelt, inden de får konsekvenser for borgerne. Konstateres det f.eks., at et IT-systems fuldautomatiske funktioner fører til, at der træffes ulovlige forvaltningsafgørelser over for borgerne, skal myndigheden straks rette

fejlene i systemet eller manuelt afhjælpe disse, inden de påvirker borgerne, eller undlade at anvende den pågældende del af systemet, indtil fejlene er rettede. Tilsvarende gælder, hvis systemet ulovligt iværksætter tvangsskridt eller f.eks. yder forkert eller misvisende vejledning om borgernes retsstilling.

Hvis et IT-system omvendt begår fejl, der alene har ordensmæssig betydning eller påvirker myndighedens ressourceanvendelse, eller fejl, som kan afhjælpes, inden de fører til ulovlige afgørelser eller øvrige ulovlige skridt over for borgerne, fører dette ikke til, at myndigheden skal undlade at anvende systemet. Sidstnævnte type af fejl indebærer dog en generel risiko for, at der i hyppigere omfang end i øvrigt opstår (manuelle) fejl. Disse fejl ved systemerne skal derfor rettes snarest muligt.«

Med andre ord lagde Kammeradvokaten til grund, at en forvaltningsmyndighed har pligt til at sikre udbedring eller standse brugen af et sagsbehandlende it-system, hvis der konstateres fejl og mangler af betydning for overholdelse af lovgivningen under behandlingen af borgernes sager. Idet dette virker ganske oplagt og SKAT desuden efterfølgende og med store omkostninger til følge lukkede EFI ned i en kontrolleret proces, synes det af Kammeradvokaten anførte standpunkt at være blevet accepteret som udtryk for gældende ret af i hvert fald denne, danske forvaltningsmyndighed.

Opsummerende må det antages, at der på nuværende tidspunkt ikke er holdepunkter for at konkludere, at den forvaltningsretlige pligt til at føre tilsyn med præfabrikerede, sagsbehandlende it-løsninger indebærer, at der skal foretages undersøgelser af systemet under normal og upåfaldende drift. Der opstår dog en reaktionspligt, hvis en myndighed, der anvender et sådant system, modtager oplysninger, giver grund til mistanke om, at systemet ikke håndterer borgernes sager lovligt og i overensstemmelse med indgåede aftaler. Som følge heraf skal myndigheden undersøge omstændighederne og afklare, om systemet har de pågældende fejl og mangler med henblik på at rette op på forholdene. Heri må nødvendigvis ligge, at myndigheden skal sikre sig indsigt i og validerbar dokumentation af systemets aktuelle programmering og funktionaliteter. Der er endvidere visse indikationer i dansk, administrativ praksis på, at en myndighed enten må undlade at anvende systemet eller sørge for, at eventuelle fejl afhjælpes, inden de får konsekvenser for borgerne, hvis det konstateres, at systemets programmering fører til, at myndigheden handler ulovligt over for borgerne.

#### 4. Opsummering og konklusion

I dag udbydes sagsbehandlende it-systemer i vidt omfang som færdigudviklede løsninger til de danske forvaltningsmyndigheder – det vil sige som »hyldevarer«. Systemerne udvikles, drives, vedligeholdes og serviceres normalt af private virksomheder. I denne artikel er det blevet undersøgt, om den almindelige, danske forvaltningsret stiller krav til myndighedernes viden om og indsigt i disse it-løsninger.

Konklusionen er, at de almindelige principper om forvaltningsmyndigheders pligt til at føre tilsyn med eksterne leverandører indebærer, at danske forvaltningsmyndigheder generelt skal have en vis viden om og indblik i de sagsbehandlende it-løsninger, som anvendes til at håndtere borgernes sager. Myndighederne skal således sikre sig en vis indsigt i de præfabrikerede, sagsbehandlende it-løsnings programmering og funktionaliteter, inden systemerne tages i brug. Derudover skal myndigheden reagere ved modtagelse af oplysninger, der giver grund til mistanke om, at systemet ikke håndterer borgernes sager lovligt, korrekt og i overensstemmelse med eventuelle

aftalte kvalitetsstandarder. I denne reaktionspligt ligger først og fremmest en pligt til at undersøge forholdet nærmere. Såfremt udfaldet af en sådan undersøgelse bliver, at systemet ikke lever op til den relevante lovgivning, må myndigheden endvidere antages at være forpligtet til at sikre, at dette ikke får konsekvenser for borgerne og i øvrigt få problemet afhjulpet på hensigtsmæssig vis.

Respekteres de beskrevne principper, bør de danske myndigheder kræve – og opnå – en øget viden om og indsigt i deres egne it-løsninger i de kommende år i takt med den mere udbredte brug af it-systemer med indbyggede sagsafgørende elementer. I lyset af de indledningsvis beskrevne udmeldinger fra danske myndigheder i 2015 er der nok et stykke vej til realisering af det ligeledes nævnte forslag til en retsikkerhedsgaranti lydende på myndighedernes fulde adgang til og indsigt i de kontraherende virksomheders sagsbehandlingsprogrammer. Omvendt er det ikke urealistisk, at en afsnittende virkning fra persondataretten vil udmønte sig i øgede krav til også de på forhånd udviklede, sagsbehandlede it-løsninger. En sådan udvikling behøver ikke nødvendigvis ske ved vedtagelse af formel lovgivning, idet kravene kan udvikles som led i god forvaltningsskik. Det er eksempelvis ikke usandsynligt, at myndighederne bliver pålagt at kræve, at it-leverandører inden kontraktsindgåelse tilvejebringer validerbar eller endda valideret dokumentation af de sagsbehandlede systemers indarbejdelse af og overholdelse af relevant lovgivning.

## Noter

1. Tak til Karsten Naundrup Olesen, Carsten Henriksen og Bent Ole Gram Mortensen for bemærkninger til og drøftelser vedrørende et udkast til denne artikel. Ansvar for mangler og fejl-vurderinger i den endelige udgave påhviler naturligvis forfatteren alene.
2. For en drøftelse af sagsbehandlede it-systemer, der udvikles til at løse specifikke opgaver for en enkelt forvaltningsmyndighed, se Motzfeldt, Hanne Marie (2016) »Udvikling af it-løsninger – om delegation og digital forvaltning« *Juristen* (1): 31–40.
3. *Anbefalinger til styrkelse af sikkerheden i statens outsourcete it-drift* Digitaliseringsstyrelsen og Center for Cybersikkerhed, 2014, forordet.
4. Henriksen, Carsten (2004) 2004) *Rammebetingelser for udlicitering af myndighedsopgaver* Responsum til Udliciteringsrådet, s. 24 og 40, tilgængeligt på <http://www.fm.dk/publikationer/2004/rammebetingelser-for-udlicitering-af-myndighedsopgaver>.
5. EFI stod for Et Fælles Inddrivelsessystem og var ikke en af de omtalte hyldevarer, men en løsning der blev udviklet særligt til RIM, der er den danske skatteforvaltnings inddrivelsesmyndighed (RestanceInddrivelsesMyndigheden), information tilgængelig på <http://www.skat.dk/SKAT.aspx?oId=71150>, senest besøgt den 26. maj 2016.
6. Skatteministeriet. (2015) *Skat ud af krisen – et oplæg til politisk samling*, s. 5, tilgængelig på <http://www.skm.dk/media/1263581/Skat-ud-af-krisen.pdf>, senest besøgt den 26. maj 2016.
7. Besvarelse af Folketingets Retsudvalg spørgsmål nr. 114 af 15. december 2015 (Alm del), tilgængeligt på <http://www.ft.dk/samling/2015/alm-del/reu/spm/114/svar/1299519/1599504.pdf>, senest tilgået 26. maj 2016.

8. KMDs digitale publikationer, tilgængelig på: [http://publikationer.kmd.dk/#SKI/02.19%20ASP%20-%20CLOUD/!](http://publikationer.kmd.dk/#SKI/02.19%20ASP%20-%20CLOUD/), senest besøgt den 26. maj 2016.
9. Folketingets Ombudsmands notat om forvaltningsretlige krav til det offentlige it-løsninger (2016), s. 1, tilgængeligt på [http://www.ombudsmanden.dk/om/formidling\\_og\\_viden/publikationer/notater/it-notat\\_januar\\_2016/](http://www.ombudsmanden.dk/om/formidling_og_viden/publikationer/notater/it-notat_januar_2016/). Se også *Justitsministeriets notat om forvaltningsretlige krav til det offentlige it-løsninger* af 18. november 2015, s. 2, ikke aktuelt tilgængeligt på Digitaliseringsstyrelsens hjemmeside, men er tilgængeligt: <http://webcache.googleusercontent.com/search?q=cache:irH1qn1lluJ:www.digst.dk/~media/Files/Digitaliseringsstrategien/Notat-om-forvaltningsretlige-krav-til-det-offentliges-it-løsninger.pdf+&cd=2&hl=da&ct=clnk&gl=dk&client=firefox-b>, senest besøgt den 26. maj 2016.
10. Henrichsen, Carsten (2015) »Administrative sanktioner som retshåndhævelsesmiddel – en introduktion« i Henrichsen, Carsten og Pagh, Peter (red): *Smæk for skillingen. Retsvidenskabelige studier i administrative sanktioner*. Jurist- og Økonomforbundets forlag, s. 33. Samme i (2014) *Dansk Kommunalret – grundtræk af den kommunale styrelseslovgivning*, s. 42 og 157. Se desuden note 2, s. 39 og Revsbech, K. (2014). *Forvaltningsret Sagsbehandling*. Jurist- og Økonomforbundets forlag, s. 68 og samme (2015) *Kommunernes opgaver, Kommunalfuldmagten mv.* Jurist og Økonomforbundets Forlag, s. 321 ff.
11. Lovforslag nr. 65 af 24. februar 2005 om regioner og om nedlæggelse af amtskommunerne, Hovedstadens Udviklingsråd og Hovedstadens Sygehusfællesskab, bemærkningerne til § 5, stk. 2.
12. For god ordens skyld oplyses det, at forfatteren til nærværende artikel var sagsbehandler på sagen i sin daværende funktion af fuldmægtig for den danske ombudsmand.
13. Se note 9, s. 1.
14. Lovbekendtgørelse nr. 1052 af 8. september 2015 med senere ændringer. Lovens § 16, stk. 1, lyder sådan: »Kommunalbestyrelsen har pligt til at føre tilsyn med, hvordan de kommunale opgaver løses, jf. § 15. Tilsynet omfatter både indholdet af tilbudene og den måde, opgaverne udføres på.»
15. Lovforslag nr. 228 af 16. april 1997 om lov om retssikkerhed og administration på det sociale område, Almindelige bemærkninger, pkt. 7 om kommunalbestyrelsens og amtsrådets pligt til at føre tilsyn.
16. Se om kravene Motzfeldt, Hanne Marie. (2015) »Den danske ombudsmands krav om værdibaseret design af den digitale forvaltning« *Nordisk Administrativ Tidsskrift* (3): 8–23.
17. Tilsvarende synes forudsat i Naundrup Olesen, Karsten (2011) *Offentlig opgave på kontrakt* Jurist og Økonomforbundets forlag, især s. 96 f, men også 64 ff og 101. Meget overordnet om spørgsmålet; Mathiassen, Jørgen. (1974) *Aftaler i forvaltningsretten med særlig henblik på aftaler mellem forvaltningsmyndigheder og private*, Juristforbundets forlag, s. 597 ff.
18. Eksempelvis Henrichsen, Carsten (2014) *Dansk Kommunalret – grundtræk af den kommunale styrelseslovgivning*, Ex Tuto, s. 155 sammenholdt med s. 157.
19. Der sigtes til følgende passage: »Det gælder for opgaver, der udføres af kommunens eller amtskommunens eget personale, og for opgaver udført af andre.« Tilsvarende om tilsyn med opgaveudførelse efter delegation mellem kommuner: Engberg, Morten. (2014) »Forpligtende kommunale samarbejder« Blume, Peter (red.) & Carsten Henrichsen (red.): *Forvaltning og retssikkerhed, Festskrift til Steen Rønsholdt* Jurist og økonomforbundets forlag, s. 152 f og 156 f.
20. Lov nr. 117 af 15. april 1964 med senere ændringer. Bestemmelsen lyder sådan: »§ 3. Ved anvendelsen af borgerlig straffelovs regler om ansvar for medvirken til en lovovertrædelse skal en minister anses for medvirkende til en underordnet handling, når 1) han har været bekendt med, at den pågældende handling ville blive foretaget, og har undladt at søge dette hindret. 2) handlingen har været et nødvendigt eller naturligt middel til gennemførelse af en beslutning, for



- hvilken ministeren er ansvarlig. 3) han har fremmet handlingens udførelse ved ikke i rimeligt omfang at føre tilsyn og fastsætte instrukser.«
21. Christensen, Jens Peter m.fl. (2002) *Undersøgelseskommissioner, Embedsmandsansvaret & Folketingets Rolle med kommentarer*, Jurist- og Økonomforbundets forlag, s. 280. Samme i (1998) *Offentlig ansatte chefers ansvar – en udredning om visse forhold af betydning for offentlig ansatte chefers retsstilling*, Finansministeriet, s. 47 ff.
  22. Beretning afgivet af Statsløsekommissionen (2015), s. 190, tilgængelig via <http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2015/statsl%C3%B8sekommissionen-har-i-dag-afgivet-sin-beretning>, senest besøgt den 26. maj 2016. Se tilsvarende (2014) Redegørelse til Forsvarsudvalget af 14. januar 2014, Forsvarsudvalgets bilag 60, Alm. del, 2013-14, journalnummer 7507821 *Det retlige grundlag for vurdering af embedsmænds ansvar*, tilgængelig på <http://www.ft.dk/samling/20131/alm-del/fou/bilag/60/1328842.pdf>, senest besøgt den 26. maj 2016.
  23. Se note 14.
  24. Bønsing, Sten (2016), »Embedsmænds pligter – en kommentar til »Kodex VII – Syv centrale pligter for embedsmænd i centraladministrationen««, UfR 2016B.33.
  25. Lovbekendtgørelse nr. 488 af 06 maj 2010 med senere ændringer.
  26. Lovbekendtgørelse nr. 873 af 9. juli 2015 med senere ændringer.
  27. John Klausen, John. Von Hielmcrone, Nina og Schultz, Trine (2012) »Delegation af myndighedsudøvelse til private« i i Munk Hansen, Carsten & Schultz, Trine (red.): *Retssikkerhed i konkurrence med andre hensyn* Jurist- og Økonomforbundets forlag, s. 73 ff med omfattende videre henvisninger. Senere udgivet er eksempelvis Karsten Revsbech m.fl., *Forvaltningsret sagsbehandling*, 7. udg., DJØF, 2014, s. 67 ff eller Sten Bønsing, *Almindelig Forvaltningsret*, 3. udg., DJØF, 2013, s. 27.
  28. Henrichsen, Carsten (2004) *Udlicitering af myndighedsopgaver – er det foreneligt med retssikkerhedsmæssige hensyn* i Henrichsen, Carsten, Rønsholdt, Steen og Blume, Peter (red.): *Forvaltningsretlige perspektiver*, Jurist- og Økonomforbundets forlag, s. 434 ff.
  29. Note 24 og eksempelvis Gammeltoft Hansen, Hans m.fl. (2002) *Forvaltningsret* Jurist- og Økonomforbundets forlag, s. 145.
  30. Se i øvrigt om lovbestemt delegation i Danmark: Bønsing, Sten (2013) *Lovbestemt delegation af forvaltningsvirksomhed til private*, Juristen nr. 6, s. 263-269. Artiklen kommer dog ikke ind på spørgsmålet om tilsyn.
  31. FOB 2014-24. Se også note 7, s. 11.
  32. Lov nr. 429 af 31. maj 2000 med senere ændringer. Se om myndigheders outsourcete it-løsninger eksempelvis Datatilsynets journalnummer 2015-632-0153, Kritik af kommunes behandling af følsomme personoplysninger i it-systemet ISAP.
  33. Bekendtgørelse nr. 528 af 15. juni 2000.
  34. <https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/databehandler/>, senest besøgt den 26. maj 2016.
  35. Datatilsynets journalnummer 2010-52-0138, Behandling af følsomme personoplysninger i cloud-løsning.
  36. Besvarelse af Folketingets Retsudvalgs spørgsmål nr. 25 af 13. oktober 2014 (Alm del), tilgængelig på <http://www.ft.dk/samling/20141/alm-del/reu/spm/25/svar/1184599/1439409.pdf>.
  37. Datatilsynets journalnummer 2011-631-0136, KL's overførsel af køreprøvesystem til en cloud-løsning.
  38. Ekstern it-revision er nævnt som en mulighed i bemærkningerne til § 7 i vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

39. Europa-Parlamentets og Rådets Forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
40. I en række tilfælde vil der desuden skulle foreligge en konsekvensanalyse efter persondataforordningens artikel 35, før myndighederne må behandle oplysninger i de sagsbehandlende it-løsninger.
41. Se også om sagen Motzfeldt, Hanne Marie (2016) »Processuelle krav« i Gram Mortensen, Bent Ole (red.): *Erhvervsforvaltningsret* Jurist og Økonomforbundets forlag, s. 178 f.
42. For så vidt angår overtilsyn med informationssikkerhed inden for et ministerområde, se Digitaliseringsstyrelsens vejledning om Departementets tilsyn med informationssikkerheden på ministerområdet <http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Koncept-for-tilsyn-med-informationssikkerhed-i-staten>.
43. I FOB 2010 20-14 står: ”Kommunen har således efter omstændighederne pligt til at undersøge sagen nærmere hvis den, f.eks. gennem en klage, får oplysninger som viser at det ikke er usandsynligt at den kommunale leverandør har tilsidesat sin forpligtelse efter de indgåede aftaler.” Understregning foretaget her.
44. Tilsvarende praksis findes ikke for aftalte standarder som eksempelvis driftssikkerhed eller brugervenlighed.
45. Kammeradvokaten er ikke en offentlig myndighed, men et privat advokatfirma, der gennem Finansministeriet har aftale med staten om at levere advokatydelse til centraladministrationen.
46. <http://www.skm.dk/media/1263555/Kammeradvokatens-notat-om-SKATs-anvendelse-af-%C3%89t-Faelles-Inddrivelsessystem.pdf>, senest besøgt den 27. maj 2016.