FOU nr 2013.0017 (Gældende)

2013-17. Oplysninger om NemID kunne ikke undtages fra aktindsigt af hensyn til statens sikkerhed

Ministerium: Folketinget

2013-17. Oplysninger om NemID kunne ikke undtages fra aktindsigt af hensyn til statens sikkerhed

En journalist klagede over, at Finansministeriet og Digitaliseringsstyrelsen havde undtaget nogle oplysninger, da han fik aktindsigt i to systemrevisionserklæringer for NemID.

Myndighederne havde undtaget oplysningerne efter offentlighedslovens § 13, stk. 1, nr. 1, om væsentlige hensyn til statens sikkerhed eller rigets forsvar.

På det generelle plan erklærede ombudsmanden sig enig i, at oplysninger af betydning for sikkerheden omkring NemID kan være af en sådan karakter, at aktindsigt vil kunne begrænses med henvisning til nødvendig beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar.

Efter at have gennemgået de oplysninger, som konkret var blevet undtaget fra aktindsigt, kunne ombudsmanden imidlertid ikke anerkende, at betingelserne for at undtage disse oplysninger med henvisning til statens sikkerhed var opfyldt. Ombudsmanden mente ikke, at myndighederne nærmere havde forklaret, hvordan sådanne skadevirkninger kunne indtræde, som forudsættes efter bestemmelsen i offentlighedslovens § 13, stk. 1, nr. 1. På den baggrund henstillede ombudsmanden til Finansministeriet at genoptage sagen og træffe en ny afgørelse.

Ombudsmanden modtog senere underretning om, at Digitaliseringsstyrelsen havde truffet en ny afgørelse i sagen, hvorved journalisten fik fuld aktindsigt i de to systemrevisionserklæringer for NemID, som sagen handlede om.

(J.nr. 13/00087)

I sin afsluttende udtalelse til journalisten skrev ombudsmanden følgende:

”1. Afgrænsning af min undersøgelse

Sagen handler om to systemrevisionserklæringer for NemID: systemrevisionserklæring af 27. april 2010, som blev afgivet før idriftsættelsen af NemID den 1. juli 2010, og systemrevisionserklæring af 24. januar 2011, som vedrører perioden fra 24. april 2010 og året ud.

Du har bedt om at få en fuldstændig kopi af erklæringerne, men Finansministeriet og Digitaliseringsstyrelsen har, i forbindelse med at du blev meddelt aktindsigt i erklæringerne, undtaget visse oplysninger.

Digitaliseringsstyrelsen begrundede oprindeligt undtagelserne med henvisning til offentlighedslovens § 13, stk. 1, nr. 6, set i lyset af § 13, stk. 1, nr. 4 (sådan må jeg forstå henvisningerne i afgørelsen). Finansministeriet tilføjede i sin afgørelse af klagesagen en henvisning til offentlighedslovens § 13, stk. 1, nr. 1. Ministeriet har siden udtalt, at det efter ministeriets opfattelse er rigtigst at henvise til den sidstnævnte bestemmelse som begrundelse for at undtage oplysninger fra din aktindsigt i de to systemrevisionserklæringer for NemID, som sagen handler om.

I lyset af Finansministeriets endelige begrundelse har jeg koncentreret min undersøgelse om spørgsmålet om undtagelse af de pågældende oplysninger med henvisning til, at det var nødvendigt af hensyn til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar, jf. offentlighedslovens § 13, stk. 1, nr. 1. Jeg forstår således Finansministeriets tilkendegivelser på den måde, at bestemmelserne i lovens § 13, stk. 1, nr. 4 og 6, efter ministeriets opfattelse ikke kan finde anvendelse, og jeg har derfor ikke anledning til at komme nærmere ind på disse bestemmelser.

Om NemID og systemrevision

NemID er en digital signatur, dvs. en elektronisk underskrift, som har til formål at sikre, at brugeren er den, som den pågældende giver sig ud for at være, når vedkommende skriver under i forbindelse med elektronisk kommunikation. NemID giver brugeren mulighed for at anvende det samme bruger-id og den samme adgangskode til både netbank, offentlige hjemmesider og en række private tjenester på nettet. NemID er udviklet af Nets DanID og blev lanceret den 1. juli 2010.

Flere oplysninger om NemID kan bl.a. findes på Digitaliseringsstyrelsens hjemmeside, www.digst.dk, og på www.nemid.nu, hvor der også er en række overordnede oplysninger om teknikken og sikkerheden i systemet.

Digital signatur, og dermed NemID, er i Danmark ikke underlagt detaljeret lovgivning, men reguleres i høj grad af såkaldte OCES-certifikat-politikker, som bl.a. fastsætter kvalitetskrav til udstederne af digital signatur, herunder Nem-ID. OCES står for "Offentlige Certifikater til Elektronisk Service". Kravene i certifikatpolitikkerne er dog i et vist omfang baseret på lov om elektroniske signaturer (jf. lov nr. 417 af 31. maj 2000 med senere ændringer), og de indeholder bl.a. krav til certifikaternes indhold, krav til udstedelse af certifikater og krav til certificeringscentrets sikkerhed. Desuden skal certificeringscentret formulere en erklæring om, hvordan centret vil leve op til kravene i certifikatpolitikken. Erklæringen danner grundlag for en ekstern revision af certificeringscentrets praksis i forbindelse med drift af og sikkerhed omkring certifikatet.

Digitaliseringsstyrelsen har særligt i forhold til NemID oplyst, at Nets DanID har udviklet og driver systemet bag den offentlige digitale signatur, NemID, for den offentlige sektor, og at Nets DanID i den forbindelse har indgået en OCES-standardaftale med Digitaliseringsstyrelsen, hvori Nets DanID har forpligtet sig til at overholde kravene i OCES-certifikatpolitikken.

Digitaliseringsstyrelsen har også oplyst, at Nets DanID i henhold til certifikatpolitikken er underlagt et tilsyn. Tilsynet har til formål at kontrollere, at Nets DanID's systemer og processer omkring pålidelige systemer, udstedelse af certifikater (digitale signaturer, f.eks. NemID) m.v. lever op til OCES-certifikatpolitikken. Tilsynet varetages af Digitaliseringsstyrelsen og er ifølge styrelsen baseret på Nets DanID's egen rapportering, på ledelseserklæringer fra Nets DanID og på ekstern systemrevision foretaget af en statsautoriseret revisor udmøntet ved revisionserklæringer mv. Det er to sådanne eksterne revisionserklæringer, som denne sag handler om.

På www.nemid.nu udgives månedlige statistikrapporter om anvendelsen af NemID. Af rapport nr. 06-2013 med kørselsdato den 3. juli 2013 fremgår, at antallet af NemID med offentlig digital signatur i juni 2013 var 3.900.000 og det samlede antal NemID i alt 4.130.000. Det fremgår desuden, at antallet af månedlige transaktioner i maj 2013 var tæt på 50.000.000. Anvendelsen af NemID er således overordentlig udbredt i Danmark.

Dette har sammenhæng med den fællesoffentlige digitaliseringsstrategi 2011-2015, som regeringen, Kommunernes Landsforening og Danske Regioner indgik aftale om i august 2011. Det er et af strategiens mål, at det for borgerne frem mod 2015 vil blive obligatorisk at bruge de digitale løsninger i deres skriftlige kommunikation med de offentlige myndigheder. Digitaliseringsstrategiens mål understøttes af lovgivning – se f.eks. lov nr. 558 af 18. juni 2012 om ændring af lov om Det Centrale Personregister, lov om dag-, fritids- og klubtilbud m.v. til børn og unge, lov om folkeskolen og sundhedsloven (Overgang til obligatorisk digital selvbetjening for borgere, for så vidt angår anmeldelse af flytning, ansøgning om plads i dagtilbud, indskrivning i folkeskole og skolefritidsordning samt ansøgning om sundhedskort og EU-sygesikringskort).

Generelt om undtagelse af oplysninger fra aktindsigt efter offentlighedslovens § 13, stk. 1, nr. 1

Som nævnt indledningsvist har Finansministeriet (endeligt) henvist til offentlighedslovens § 13, stk. 1, nr. 1 (lov nr. 572 af 19. december 1985 med senere ændringer) i begrundelsen for at undtage visse oplysninger fra din aktindsigt i de to systemrevisionserklæringer. Efter ministeriets opfattelse vil videregivelse af de undtagne oplysninger kunne have alvorlige sikkerhedsmæssige konsekvenser af en sådan karakter, som er omfattet af bestemmelsens beskyttelseshensyn.

Bestemmelsen i offentlighedslovens § 13, stk. 1, nr. 1 (og stk. 2) lyder sådan:

'§ 13. Retten til aktindsigt kan begrænses i det omfang, det er nødvendigt til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar,

(…)

Stk. 2. Gør hensyn som nævnt i stk. 1 sig kun gældende for en del af et dokument, skal den pågældende gøres bekendt med dokumentets øvrige indhold. '

Bestemmelsen forudsætter, at der i hvert enkelt tilfælde foretages et konkret skøn over, hvorvidt retten til aktindsigt bør vige for væsentlige hensyn til 'statens sikkerhed eller rigets forsvar'. Aktindsigt kan kun afslås, hvor der er nærliggende fare for, at de angivne interesser vil lide skade af betydning. Se betænkning nr. 1510/2009 om offentlighedsloven, bind 2, s. 658, og John Vogter, Offentlighedsloven med kommentarer, 3. udgave (1998), s. 232 f.

Af betænkning nr. 1510/2009 om offentlighedsloven, bind 2, s. 664, fremgår om bestemmelsens anvendelsesområde i praksis bl.a. følgende:

'Det kan i øvrigt oplyses, at bestemmelsen i § 13, stk. 1, nr. 1, i forvaltningsmyndighedernes praksis er anvendt til at undtage oplysninger fra retten til aktindsigt af hensyn til beskyttelse af statsministerens personlige sikkerhed, til beskyttelse af udsendt ambassadepersonales sikkerhed samt operationssikkerhed for udsendte militære styrker. Herudover er bestemmelsen anvendt til at undtage bestemte oplysninger af hensyn til et ministeriums IT-sikkerhed, hvilket i øvrigt er anerkendt af ombudsmanden i en utrykt udtalelse af 9. maj 2007. '

I den utrykte ombudsmandsudtalelse, som er nævnt i citatet fra betænkning nr. 1510/2009, fandt ombudsmanden ikke grundlag for at kritisere, at Statsministeriet havde givet afslag på aktindsigt i navnet på en bestemt it-virksomhed med henvisning til ministeriets it-sikkerhed.

Statsministeriet havde oplyst, at den pågældende virksomhed og dens produkter spillede en afgørende rolle for Statsministeriets it-sikkerhed, og at en offentliggørelse af virksomhedens navn ville svække ministeriets it-sikkerhed. Statsministeriet pegede i den forbindelse bl.a. på, at jo smallere produktlinje en virksomhed kan tilbyde inden for it-sikkerhed, jo mere betydningsfuldt er det at kunne tilbageholde oplysninger om samarbejdet med den pågældende virksomhed. Ombudsmanden kunne i den konkrete sag ikke vurdere skadevirkningerne på en anden og bedre måde end Statsministeriet, fordi en kontrol af de it-sikkerhedsmæssige vurderingers rigtighed, som var af afgørende betydning for sagen, krævede en fagkundskab, som ombudsmanden ikke havde.

Finansministeriets afgørelse om undtagelse af oplysninger fra aktindsigt efter offentlighedslovens § 13, stk. 1, nr. 1, og min vurdering

Finansministeriet tiltrådte den 1. maj 2012 Digitaliseringsstyrelsens afgørelse af 12. januar 2012 om at undtage enkelte afsnit i de eksterne systemrevisionserklæringer for NemID af 27. april 2010 og 24. januar

2011 fra aktindsigt. Som beskrevet under punkt 1 ovenfor blev undtagelserne (endeligt) begrundet med henvisning til offentlighedslovens § 13, stk. 1, nr. 1.

I systemrevisionserklæringen af 27. april 2010 blev teksten under første og sidste 'bullet' på side 2 undtaget fra aktindsigt. I systemrevisionserklæringen af 24. januar 2011 blev teksten i afsnittet under overskriften 'Supplerende oplysninger' øverst på side 2 undtaget.

Finansministeriet og Digitaliseringsstyrelsen har i deres afgørelser og udtalelser (se nærmere i den vedlagte sagsfremstilling) bl.a. anført følgende om, hvorfor det var nødvendigt at undtage de pågældende tekststykker fra aktindsigt:

- '[O]ffentliggørelse af de udeladte oplysninger vil kunne have alvorlige sikkerhedsmæssige konsekvenser. '

- 'Det er af afgørende betydning for sikkerheden i systemet, og dermed tilliden til systemet, at systemets tekniske og sikkerhedsmæssige indretning og procedurerne heromkring ikke offentliggøres. Samtidig er det en forudsætning for, at Digitaliseringsstyrelsen kan føre det nødvendige tilsyn, at disse oplysninger indgår i den årlige rapportering. '

- '[D]er er […] ikke noget hensyn, der tilsiger, at borgerne skal være bekendt med de mere specifikke tekniske indretninger og sikkerhedsmæssige procedurer, som er med til at skabe sikkerheden, og som derfor indgår i tilsynsrapporteringen. '

- '[B]orgerne [vil] potentielt […] blive udsat for unødvendige risici, hvis oplysninger om findings […] bliver offentliggjort. '

På det generelle plan er jeg enig i, at oplysninger af betydning for sikkerheden omkring NemID kan være af en sådan karakter, at aktindsigt vil kunne begrænses med henvisning til nødvendig beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar, jf. offentlighedslovens § 13, stk. 1, nr. 1. Et sikkerhedsproblem i forhold til NemID vil således kunne få alvorlige konsekvenser, bl.a. som følge af den meget udbredte anvendelse af NemID i Danmark i dag (se afsnit 2 ovenfor).

For at undtage oplysninger efter bestemmelsen i offentlighedslovens § 13, stk. 1, nr. 1, forudsættes det imidlertid, at de mulige skadevirkninger ved at udlevere *bestemte* oplysninger efter en *konkret* vurdering må anses for at være tilstrækkeligt tungtvejende. Jeg henviser til det, som jeg har redegjort for i afsnit 3 ovenfor om anvendelsen af § 13, stk. 1, nr. 1.

Jeg har gennemgået de tekstafsnit i de to systemrevisionserklæringer for NemID, som myndighederne har undtaget fra aktindsigt. Min gennemgang giver mig anledning til følgende bemærkninger:

Myndighedernes afgørelser og udtalelser giver indtryk af, at de udeholdte afsnit indeholder oplysninger om 'systemets tekniske og sikkerhedsmæssige indretning og procedurerne heromkring', 'specifikke tekniske indretninger og sikkerhedsmæssige procedurer' og 'oplysninger om findings'.

Hertil skal jeg bemærke, at jeg efter en gennemgang af de udeholdte linjer i dokumenterne kan konstatere, at der ikke heri findes *konkrete* oplysninger af den beskrevne karakter. De nævnte citater fra myndighedernes afgørelser og udtalelser er derfor efter min opfattelse ikke dækkende. De udeholdte linjer indeholder, så vidt jeg kan vurdere, alene *generelle* bemærkninger, der er udformet som kortfattede 'bullets' i afsnit om 'svagheder' ved systemet. De omtalte svagheder er ikke nærmere angivet. Der findes heller ikke nogen teknisk eller sikkerhedsmæssig beskrivelse heraf.

På den baggrund kan jeg – på det foreliggende grundlag – ikke anerkende, at betingelserne for anvendelse af bestemmelsen i § 13, stk. 1, nr. 1, er opfyldt. Myndighederne har således hverken i afgørelserne

eller i deres udtalelser til mig nærmere forklaret, hvordan sådanne skadevirkninger kan indtræde, som forudsættes for at undtage oplysninger efter bestemmelsen. Myndighederne har heller ikke oplyst noget om, at de eventuelt i fortrolighed kunne give mig en sådan forklaring.

Jeg har derfor i dag henstillet til Finansministeriet at genoptage sagen og træffe en ny afgørelse om aktindsigt under inddragelse af det, som jeg har anført ovenfor. Jeg har bedt om underretning om Finansministeriets nye afgørelse.

…"

Jeg modtog efterfølgende underretning om, at Digitaliseringsstyrelsen i forlængelse af min udtalelse havde truffet en ny afgørelse og herved givet journalisten fuld aktindsigt i de to systemrevisionserklæringer for NemID, som sagen handlede om, herunder også i de oplysninger som tidligere var blevet undtaget fra aktindsigt efter offentlighedslovens § 13, stk. 1, nr. 1.

På den baggrund foretog jeg mig ikke mere i sagen.

Sagsfremstilling

Den 5. januar 2012 anmodede en journalist, A, om aktindsigt efter offentlighedsloven i systemrevisionserklæringerne for NemID for 2010 og 2011 og i journallisten vedrørende de pågældende systemrevisionserklæringer.

Digitaliseringsstyrelsen traf afgørelse i sagen den 12. januar 2012. Styrelsen oplyste, at systemrevisionserklæring for 2011 endnu ikke forelå. Styrelsen sendte derfor A kopi af de to systemrevisionserklæringer, som forelå – den ene fra før idriftsættelse af NemID den 1. juli 2010 og den anden for perioden fra 24. april 2010 og året ud.

Styrelsen undtog dog visse oplysninger fra aktindsigt. I styrelsens afgørelse står der bl.a. følgende:

"Systemrevisionserklæringerne er en del af Digitaliseringsstyrelsens tilsyn med Nets DanID som udsteder af NemID. Tilsynet er baseret på udsteders og revisors udlevering af fortrolige oplysninger, om forretningsgange og drift, som styrelsen ikke kan indhente selv. Det er derfor en afgørende forudsætning for tilsynet, at disse oplysninger kan afgives i tillid til, at fortrolige oplysninger vedrørende bl.a. sikkerheden i systemet ikke offentliggøres. På denne baggrund er der derfor med henvisning til Offentlighedslovens § 13, nr. 6 set i lyset af § 13, nr. 4 foretaget enkelte ekstraheringer i erklæringerne. "

A klagede over Digitaliseringsstyrelsens afgørelse til Finansministeriet. Ministeriet tiltrådte den 1. maj 2012 – efter at have indhentet en udtalelse i anledning af A's klage fra styrelsen – styrelsens afgørelse om at undtage visse oplysninger i erklæringerne fra aktindsigt. Ministeriets afgørelse indeholder bl.a. følgende:

"Digitaliseringsstyrelsen har i udtalelsen af 29. februar 2012 anført, at DanID A/S, på baggrund af et EU-udbud og en herefter indgået kontrakt med It- og Telestyrelsen (nu Digitaliseringsstyrelsen) har udviklet og driver systemet bag den offentlige digitale signatur, NemID, for den offentlige sektor. For at kunne udstede den offentlige digitale signatur i henhold til OCES-standarden, som er udmøntet i OCES-certifikatpolitik for personcertifikater har DanID desuden indgået en særkilt OCES-standard-aftale med Digitaliseringsstyrelsen. I denne aftale har DanID forpligtet sig til at overholde kravene i certifikatpolitikken. For at kontrollere, at DanIDs systemer og processer omkring pålidelige systemer, udstedelse af certifikater (digitale signaturer) m.v. lever op til kravene i Certifikatpolitikken er DanID i henhold til certifikatpolitikkens pkt. 5.4 underlagt et tilsyn, som varetages af Digitaliseringsstyrelsen. Tilsynet er dels baseret på DanIDs egen rapportering, dels på ledelseserklæringer fra DanID og ekstern systemrevision foretaget af en ekstern statsautoriseret revisor udmøntet ved revisionserklæringer m.v.

Styrelsen anfører videre, at det er af afgørende betydning for sikkerheden i systemet, og dermed tilliden til systemet, at systemets tekniske og sikkerhedsmæssige indretning og procedurerne heromkring ikke offentliggøres. Samtidig er det en forudsætning for, at styrelsen kan føre det fornødne tilsyn, at disse oplysninger indgår i den årlige rapportering.

Det i certifikatpolitikken etablerede tilsynssystem skal netop sikre, at sikkerheden ved NemID opretholdes, og at borgerne derfor kan stole på NemID. Dette har naturligvis interesse for offentligheden. Der er derimod ikke noget hensyn, der tilsiger, at borgerne skal være bekendt med tekniske indretninger og sikkerhedsmæssige procedurer, som er med til at skabe sikkerheden, og som derfor indgår i tilsynsrapporteringen. Styrelsen bemærker, at den overordnede tekniske indretning og arkitektur i systemet er beskrevet og offentliggjort dels på Digitaliseringsstyrelsens hjemmeside nemid.nu, dels på DanIDs hjemmeside danid.dk.

Det er Digitaliseringsstyrelsens opfattelse, at offentliggørelse af de udeladte oplysninger vil kunne have alvorlige sikkerhedsmæssige konsekvenser, og at undtagelse af oplysninger i materialet med henvisning til Offentlighedslovens § 13, nr. 6, set i lyset af § 13, nr. 4, er nødvendig for at beskytte væsentlige hensyn til private og offentlige interesser, og at hemmeligholdelse efter forholdets særlige karakter er påkrævet.

Styrelsen har på dette grundlag fastholdt sin afgørelse af 12. januar 2012.

Finansministeriet bemærker følgende:

Finansministeriet forstår Digitaliseringsstyrelsens afgørelse af 12. januar 2012 sammenholdt med styrelsens udtalelse af 29. februar 2012 således, at styrelsen i sin vurdering har lagt vægt på, at offentliggørelse af de undtagne oplysninger vil kunne have alvorlige sikkerhedsmæssige konsekvenser, og at undtagelse af oplysninger i materialet, med henvisning til offentlighedslovens § 13, stk. 1, nr. 6 set i lyset af § 13, stk. 1, nr. 4 derfor er nødvendig for at beskytte væsentlige hensyn til private og offentlige interesser, og at hemmeligholdelse efter forholdets særlige karakter er påkrævet.

Finansministeriet skal for en god ordens skyld i denne forbindelse bemærke, at Digitaliseringsstyrelsen i afgørelsen og udtalelsen ikke har henvist korrekt til offentlighedsloven, idet der burde have stået § 13, stk. 1, nr. 6 henholdsvis § 13, stk. 1, nr. 4. Ordene 'Stk. 1' mangler således begge steder. Derudover er der ikke tale om 'ekstrahering' af oplysninger, men om 'undtagelse' af oplysninger.

Finansministeriet kan tilslutte sig Digitaliseringsstyrelsens vurdering af, at offentliggørelse af de undtagne oplysninger vil kunne have alvorlige sikkerhedsmæssige konsekvenser. Finansministeriet finder ikke, at hensynet til offentlighedens interesse i sagen begrunder en fravigelse af hensynet til beskyttelse af det offentliges interesser. Finansministeriet finder endvidere, at der, ud over den af Digitaliseringsstyrelsen anvendte begrundelse, kunne have været henvist til offentlighedslovens § 13, stk. 1, nr. 1, hvorefter retten til aktindsigt kan begrænses i det omfang det er nødvendigt til beskyttelse af væsentlige hensyn til statens sikkerhed.

På baggrund af ovenstående finder Finansministeriet således ikke grundlag for at ændre Digitaliseringsstyrelsens afgørelse. "

A klagede til mig over Finansministeriets afgørelse i et klageskema af 3. januar 2013. I klagen pegede A på, at det efter hans opfattelse ikke er muligt at give en korrekt dækning af sagen, når essentielle elementer i erklæringerne er udeladt. A mente, at eventuelle problemer med den digitale signatur, som det er tanken, at alle borgere skal benytte, bør komme frem i lyset, navnlig fordi der flere gange har været sat spørgsmålstegn ved sikkerheden i forbindelse med NemID. Hensynet hertil bør efter A's opfattelse

veje tungere end de hensyn, som myndighederne havde lagt vægt på, da oplysninger blev undtaget fra aktindsigt.

Jeg bad den 18. januar 2013 Finansministeriet og Digitaliseringsstyrelsen om udtalelser om sagen, og jeg modtog udtalelserne den 19. april 2013. I Digitaliseringsstyrelsens udtalelse af 10. april 2013 står der:

"Digitaliseringsstyrelsen henholder sig fortsat til den tidligere afgørelse i sagen og bemærkninger fremsendt til Finansministeriet den 29. februar 2012 i forbindelse med (A)'s klage over Digitaliseringsstyrelsens afgørelse af 12. januar 2012.

Herudover kan Digitaliseringsstyrelsen specifikt i forhold til det af (A) i klagen til Folketingets Ombudsmand anførte bemærke:

1. Ingen it-systemer kan laves med 100% sikkerhed. Det betyder, at udover den tekniske og sikkerhedsmæssige arkitektur i systemet, opretholdes det høje sikkerhedsniveau ved løbende overvågning af trusler, løbende iværksættelse af tiltag over for nye sårbarheder, løbende overvågning af systemet og detaljerede procedurer for hele denne proces.

2. Digitaliseringsstyrelsen er enig i, at den offentlige kontrol (tilsynet) foretages for borgernes skyld og for at varetage offentlige interesser. Det er derimod styrelsens klare overbevisning, at borgerne potentielt vil blive udsat for unødvendige risici, hvis oplysninger om findings i forbindelse med kontrol og tilsyn med de ovenfor beskrevne forløb og procedurer bliver offentliggjort. Borgernes interesser varetages ved, at tilsynet sikrer, at Nets DanID hele tiden overholder kravene i OCES-certifikatpolitikkerne og løbende følger op på sikkerheden i systemet. "

Finansministeriet udtalte sig bl.a. sådan:

"Finansministeriet kan henholde sig til ministeriets afgørelse af 1. maj 2012.

Finansministeriet kan således fortsat tilslutte sig Digitaliseringsstyrelsens vurdering af, at offentliggørelse af de undtagne oplysninger vil kunne have alvorlige sikkerhedsmæssige konsekvenser. Finansministeriet finder ikke, at hensynet til offentlighedens interesse i sagen, i det konkrete tilfælde kan begrunde en fravigelse af beskyttelsen af væsentlige hensyn til statens sikkerhed eller rigets forsvar.

Finansministeriet skal i den forbindelse supplerende bemærke, at det efter ministeriets opfattelse er rigtigst at henvise til offentlighedslovens § 13, stk. 1, nr. 1, hvorefter retten til aktindsigt kan begrænses i det omfang, det er nødvendigt til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar.

Finansministeriet kan i den forbindelse særligt henvise til Betænkning nr. 1510/2009 om offentlighedsloven, bind 2 side 664. Det fremgår her vedrørende anvendelsen af § 13, stk. 1, nr. 1:

'Herudover er bestemmelsen anvendt til at undtage bestemte oplysninger af hensyn til et ministeriums IT-sikkerhed, hvilket i øvrigt er anerkendt af ombudsmanden i en utrykt udtalelse af 9. maj 2007 (j.nr. 2007-0333-801). I den nævnte udtalelse har ombudsmanden således anerkendt, at Statsministeriet under henvisning til ministeriets IT-sikkerhed kunne afslå aktindsigt i navnet på en bestemt IT-virksomhed. Som begrundelse herfor havde Statsministeriet henvist til, at den pågældende virksomhed og dens produkter spillede en afgørende rolle for Statsministeriets IT-sikkerhed, og at en offentliggørelse af virksomhedens navn ville svække ministeriets IT-sikkerhed. '

Digitaliseringsstyrelsens udtalelse af 10. april 2013 giver ikke Finansministeriet anledning til supplerende bemærkninger. "

Jeg gjorde herefter A bekendt med myndighedernes udtalelser, og A sendte mig sine bemærkninger til dem i en e-mail af 23. maj 2013. A skrev bl.a. sådan:

"Svar på Digitaliseringsstyrelsens bemærkninger til Folketingets Ombudsmand

1. Netop fordi ingen it-systemer kan laves med 100 procent sikkerhed, er det interessant for offentligheden at vide, hvilken indsats, man har gjort for at sikre sig, at sårbarheder ikke kan udnyttes. En del af den demokratiske kontrol må derfor være, at borgerne via gennemsigtighed kan få problematiske områder oplyst – specielt når de som i tilfældet her ligger flere år tilbage og – forhåbentlig – er blevet rettet siden. Interessen for sikkerheden og konstruktionen i NemID er kun blevet større med årene – senest i en højaktuel debat om tilgængeligheden ved NemID som følge af såkaldte DDoS-angreb på tjenesten. I debatten kom det frem, at tjenesten har kørt i flere år uden at være sikret mod en af de mest almindelige angrebsformer på internettet. Derfor er det mere aktuelt end nogensinde at få indsigt i, hvilke problematikker, Nets DanID og det offentlige har stået over for for år tilbage.

1. Et af fundamenterne i demokratiet er offentlighed i forvaltningen. Derfor er jeg ikke enig i argumentet om lukkethed for borgernes egen skyld. Da jeg ikke har mulighed for at vurdere, om de udstregede passager reelt skyldes statens sikkerhed eller rigets forsvar er på spil, er det derfor også svært for mig at forholde mig yderligere til argumentet.

Svar på Finansministeriets bemærkninger til Folketingets Ombudsmand

Som følge af Folketingets Ombudsmands tilslutning til Statsministeriets ønske om at hemmeligholde navnet på en leverandør kom der blandt andet kritik af hemmeligholdelsen fra en af it-sikkerhedsbranchens mest fremtrædende personer.

I artiklen 'Ombudsmand beskytter hemmeligt it-sikkerhedsfirma' bragt 14. maj 2007 på Computerworld udtaler direktør (…) fra it-sikkerhedsfirmaet (…):

'Ud fra et fagligt synspunkt er det ikke sagligt at hemmeligholde navnet på grund af it-sikkerheden – tværtimod. '

På samme måde er Digitaliseringsstyrelsens og Nets DanIDs strategi om såkaldt security through obscurity (sikkerhed, der ligger i hemmeligholdelse) blevet kritiseret mange gange af ledende eksperter og forskere. Der er hverken en saglig eller faglig grund til at holde disse detaljer skjult. "

Jeg sendte den 6. juni 2013 A's bemærkninger videre til Finansministeriet og bad om ministeriets og Digitaliseringsstyrelsens supplerende bemærkninger. I den forbindelse bad jeg navnlig myndighederne om at forholde sig til A's bemærkninger, som jeg opfattede sådan, at A satte spørgsmålstegn ved, om der *fortsat* var grund til at undtage oplysninger i systemrevisionserklæringerne, som vedrører en periode tilbage i 2010. Jeg bad også myndighederne om at oplyse, hvilke overvejelser myndighederne havde gjort sig i forhold til eventuel meroffentlighed.

Jeg modtog myndighedernes supplerende udtalelser den 26. juni 2013. Digitaliseringsstyrelsen skrev bl.a. følgende:

"Det forhold, at oplysningerne er flere år gamle ændrer ikke ved nødvendigheden af, at fortrolige oplysninger afgivet til tilsynet ikke kan offentliggøres. Selvom de i erklæringerne udstregede forhold er tilrettet, giver bemærkningerne stadig indsigt i tekniske og sikkerhedsmæssige forhold i den samlede løsning. Statens sikkerhed og offentlighedens interesse varetages derfor bedst ved, at tilsynet kan modtage fortrolige informationer om sikkerhedsmæssige og andre forhold, således at tilsynet kan reagere herpå og derved kan virke så effektivt som muligt. Sikkerhedsmæssige detaljer i systemets drift og indretning

egner sig ikke til offentlig debat og demokratisk kontrol, men til saglig vurdering og opfølgning, hvilket er tilsynets opgave.

Ovenstående er tillige begrundelsen for, at Digitaliseringsstyrelsen ikke har fundet, at der var grundlag for at give aktindsigt baseret på princippet om meroffentlighed i Ofl. § 4, stk. 1, 2. pkt."

I Finansministeriets supplerende udtalelse står der bl.a.:

"Digitaliseringsstyrelsens udtalelse af 20. juni 2013 giver ikke Finansministeriet anledning til supplerende bemærkninger.

Finansministeriet kan fortsat tilslutte sig Digitaliseringsstyrelsens vurdering af, at offentliggørelse af de undtagne oplysninger vil kunne have alvorlige sikkerhedsmæssige konsekvenser. Finansministeriet finder ikke, at hensynet til offentlighedens interesse i sagen, i det konkrete tilfælde kan begrunde en fravigelse af beskyttelsen af væsentlige hensyn til statens sikkerhed eller rigets forsvar.

Finansministeriet henholder sig på den baggrund til ministeriets udtalelse af 19. april 2013 og afgørelse af 1. maj 2012.

Ministeriet kan endvidere oplyse, at ministeriet, i relation til princippet om meroffentlighed, jf. offentlighedslovens § 4, stk. 1, 2. pkt., har foretaget en afvejning af på den ene side de beskyttelseshensyn, der ligger til grund for undtagelsesbestemmelsen i offentlighedslovens § 13, stk. 1, nr. 1, og på den anden side den berettigede interesse, (A) må antages at have i, at anmodningen om aktindsigt imødekommes. Ministeriet har på den baggrund ikke fundet grundlag for at udlevere de pågældende oplysninger efter meroffentlighedsprincippet. "

Jeg gjorde efterfølgende A bekendt med myndighedernes supplerende udtalelser. Jeg modtog ikke yderligere bemærkninger til sagen fra A eller myndighederne.