FOU nr 2016.9667 (Gældende)

Konsulentfirmas rapporter om sikkerhedsanalyser af IT-løsninger kunne ikke undtages fra aktindsigt efter offentlighedslovens § 23 om interne dokumenter

Ministerium: Folketinget

Journalnummer: Sag nr. 16/01002

Konsulentfirmas rapporter om sikkerhedsanalyser af IT-løsninger kunne ikke undtages fra aktindsigt efter offentlighedslovens § 23 om interne dokumenter

Svar til A

14-06-2016

Sag nr. 16/01002

DSB's afslag på aktindsigt i rapporter vedrørende sikkerhedsanalyser af IT-løsninger til opbevaring og håndtering af data fra ID-kontrol ved den dansk-svenske grænse

Jeg har nu færdigbehandlet sagen.

Det er min opfattelse, at rapporterne vedrørende de udførte sikkerhedsanalyser ikke er interne dokumenter, som kan undtages fra aktindsigt efter offentlighedslovens § 23.

Jeg har på den baggrund henstillet til DSB at genoptage behandlingen af sagen og på ny tage stilling til din anmodning om aktindsigt.

En nærmere begrundelse for resultatet af min undersøgelse findes nedenfor i afsnittet "Ombudsmandens udtalelse".

Efter udtalelsen (fra s. 4) er der en gennemgang af sagens forløb.

Ombudsmandens udtalelse

1. Hvad handler sagen om?

Du har klaget over, at DSB ved afgørelse af 15. januar 2016 – som fastholdt den 26. februar 2016 – afviste at give dig aktindsigt i rapporter vedrørende sikkerhedsanalyser af IT-løsninger til håndtering og opbevaring af data fra ID-kontrol ved den dansk-svenske grænse (bl.a. fotos af relevante identifikationsdokumenter).

DSB henviste i afgørelsen til, at de omhandlede rapporter var interne dokumenter, der som udgangspunkt kunne undtages fra aktindsigt med henvisning til offentlighedslovens § 23.

DSB var desuden af den opfattelse, at rapporterne ikke var omfattet af offentlighedslovens § 26, stk. 1, og at der ikke var ekstraheringspligtige oplysninger eller faglige vurderinger i dokumenterne, som skulle udleveres efter lovens § 28 eller § 29.

DSB fandt heller ikke grundlag for at udlevere oplysningerne til dig efter princippet om meroffentlighed i offentlighedslovens § 14.

2. Retsgrundlaget – offentlighedslovens § 23

Offentlighedsloven § 23 har følgende indhold (jf. lov nr. 606 af 12. juni 2013):

"§ 23. Retten til aktindsigt omfatter ikke interne dokumenter. Som interne dokumenter anses

1) dokumenter, der ikke er afgivet til udenforstående,

(…)

Stk. 2. Dokumenter omfattet af stk. 1, der afgives til udenforstående, mister deres interne karakter, medmindre afgivelsen sker af retlige grunde, til forskningsmæssig brug eller af andre lignende grunde.

Stk. 3. (…)"

I de specielle bemærkninger til § 23 (lovforslag nr. L 144 af 7. februar 2013) er der anført bl.a. følgende:

"Bestemmelsen i *nr. 1* indebærer – i sammenhæng med stk. 2 – at ethvert dokument, der udarbejdes af en myndighed, og som ikke afgives til udenforstående, har karakter af et internt dokument. Det er således ikke en betingelse for at undtage et dokument efter nr. 1, at dokumentet indeholder overvejelser af mere foreløbig karakter, eller at det tilsigter at tjene som grundlag for myndighedens interne beslutningsproces.

…

Hvis der på et dokument, som en myndighed har modtaget fra eller afgivet til udenforstående (og som derfor ikke betragtes som internt) (…)"

I Mohammad Ahsan, Offentlighedsloven med kommentarer (2014), er der på s. 408 bl.a. anført:

"Konsulentrapporter, der udarbejdes af private konsulentfirmaer, vil som det klare udgangspunkt ikke kunne anses som interne dokumenter. Det gælder, uanset om rapporten vedrører interne forhold i myndigheden, herunder samarbejdsforholdene, omstruktureringer, organisering osv., ligesom det gælder, selvom myndigheden løbende har medvirket aktivt i forbindelse med rapportens tilblivelse og udarbejdelse. "

3. Min vurdering

Som det fremgår nedenfor af sagsfremstillingen, oplyste DSB på et møde den 30. maj 2016, at rapporterne om sikkerhedsanalyser af det anvendte system ikke er udarbejdet af DSB selv, men af en virksomhed, som har særlig ekspertise i at gennemføre tests og sikkerhedsanalyser af IT-systemer. Rapporterne er herefter sendt til DSB.

På den baggrund er det min opfattelse, at rapporterne ikke har karakter af interne dokumenter omfattet af offentlighedsloven § 23, stk. 1, nr. 1.

Jeg har herefter ikke anledning til at tage stilling til spørgsmålet om anvendelse af offentlighedslovens §§ 26, 28 og 29 i sagen.

Jeg har gjort DSB bekendt med min opfattelse, og jeg har samtidig henstillet til DSB at genoptage sagen og på ny tage stilling til din anmodning om aktindsigt.

Jeg gør opmærksom på, at jeg ikke herved har taget stilling til, om rapporterne helt eller delvist kan undtages efter andre bestemmelser i offentlighedsloven, herunder eventuelt på baggrund af det, som DSB har anført i sin udtalelse af 16. marts 2016 om, at rapporterne indeholder oplysninger, som ville kunne misbruges til konstruktion af målrettede angreb på systemet.

Jeg har skrevet til DSB, at jeg går ud fra, at DSB i forbindelse med genoptagelsen af sagen også vil inddrage, at dataene nu er slettet, jf. DSBs oplysninger i e-mail af 24. marts 2016, som er refereret nedenfor i sagsfremstillingen.

Jeg har bedt DSB om at underrette mig om resultatet af DSB's nye stillingtagen i sagen, men jeg foretager mig i øvrigt ikke mere i sagen.

Med venlig hilsen

Jørgen Steen Sørensen

Kopi til:

DSB

Sagsfremstilling

Den 10. januar 2016 bad du DSB om indsigt i bl.a. systemrevisionserklæringer eller rapporter fra sikkerhedsanalyser foretaget af DSB's eller MobilePeoples IT-løsninger vedrørende håndtering af ID-kontrol på den dansk-svenske grænse.

Den 15. januar 2016 fik du afslag på aktindsigt i rapporter fra sikkerhedsanalyser. DSB skrev bl.a. følgende i sin afgørelse:

"Det kan til din orientering oplyses, at der ikke forefindes systemrevisionserklæringer. For så vidt angår rapporter fra sikkerhedsanalyser er der tale om interne dokumenter, som er undtaget aktindsigt i medfør af offentlighedslovens § 23. De nævnte akter er ikke omfattet af offentlighedslovens § 26, stk. 1, hvorefter retten til aktindsigt uanset § 23, stk. 1, omfatter visse interne dokumenter, som foreligger i endelig form.

Endvidere er der ikke blandt de undtagne dokumenter oplysninger om sagens faktiske grundlag eller eksterne eller interne faglige vurderinger, der skal udleveres i medfør af offentlighedslovens § 28-29.

DSB har overvejet, om de undtagne dokumenter burde udleveres til dig efter princippet om meroffentlighed i offentlighedslovens § 14, stk. 1. DSB har i den forbindelse foretaget en afvejning af på den ene side de hensyn, der ligger til grund for bestemmelsen i offentlighedslovens § 23, stk. 1, nr. 1, og på den anden side den berettigede interesse, du må antages at have i, at anmodningen om aktindsigt imødekommes. DSB har på den baggrund ikke fundet grundlag for at udlevere de pågældende dokumenter. "

Du klagede den 20. januar 2016 over afgørelsen til DSB. Du skrev bl.a. følgende:

"Jeg bekræfter hermed modtagelsen af afgørelsen. Dog finder jeg på nedenstående tre punkter at den er mangelfuld.

DSB bedes behandle dette som en klage jf. offentlighedslovens (herefter OFL) § 37, stk. 2.

1) Sikkerhedsanalyserne er af DSB blevet klassificeret som interne dokumenter. Disse undtages efter OFL § 23, stk. 1. Der nævnes i afgørelsen at dokumenterne ikke er omfattet af OFL § 26, stk. 1, hvorefter der ikke gives aktindsigt.

Det er min opfattelse at dokumenterne kunne være omfattet af § 26, stk. 1, nr. 3, der 'sigter således til rapportmateriale – afhøringsrapporter, døgnrapporter, analyserapporter, besigtigelsesrapporter og inspektionsrapporter' (Betænkning om offentlighedsloven, nr. 1510/2009, kapitel 16, punkt 3.5).

Såfremt DSB vil fastholde afslaget med denne begrundelse, bør det klarlægges hvorfor § 26, stk. 1, nr. 3 ikke finder anvendelse. Jeg henviser i øvrigt til FOB 1993.203 der også omtales i betænkningen. "

DSB skrev den 22. januar 2016 til dig, at der ikke var en højere klageinstans i forhold til DSB's afgørelse om aktindsigt. DSB vejledte dig derudover om, at du havde mulighed for at indbringe sagen for Folketingets Ombudsmand eller for domstolene.

Du klagede den 22. januar 2016 til mig over DSB's afgørelse.

Eftersom DSB ikke havde forholdt sig nærmere til din klage af 20. januar 2016 – ligesom DSB ikke havde haft lejlighed til at forholde sig til det, som du anførte i klagen til mig – sendte jeg den 5. februar 2016 din klage videre til DSB med henblik på, at DSB fik mulighed for – over for dig – at forholde sig til det, som du havde anført.

DSB skrev den 26. februar 2016 bl.a. følgende til dig:

"DSB skal fastholde sit afslag på aktindsigt i sikkerhedsanalyserne. Sikkerhedsanalyserne er udelukkende udarbejdet til internt brug i DSB og er ikke med henblik på fremlæggelse for udenforstående. DSB skal supplerende bemærke, at sikkerhedsanalyserne er udarbejdet for at sikre sikkerhedsniveauet i løsningen og en offentliggørelse af indholdet af sikkerhedsanalyserne, kan potentielt udgøre en væsentlig sikkerhedsrisiko for DSB. "

Den 29. februar 2016 klagede du til mig over DSB's afslag på indsigt i rapporterne vedrørende sikkerhedsanalyserne.

Jeg bad den 4. marts 2016 DSB om en udtalelse om sagen og om at låne akterne i sagen.

DSB anførte i sin udtalelse af 16. marts 2016 bl.a. følgende:

"DSB har afslået at give A aktindsigt i DSB's dokumentation for de udførte sikkerhedsanalyser af de komponenter, der indgår i det samlede system som benyttes i forbindelse med ID kontrollen i Københavns Lufthavn og på Københavns Hovedbanegård, med henvisning til at der er tale om interne dokumenter. Disse sikkerhedsanalyser består af såvel automatiserede sårbarhedsscanninger som manuel ekspert gennemgang af f.eks. applikationskode og konfigurationsparametre.

DSB ønsker at fastholde sit standpunkt, da de omhandlede dokumenter indeholder en række detaljerede oplysninger om, hvorledes ID kontrolsystemet er konfigureret, samt hvilke netværksadresser der anvendes. Disse oplysninger vil kunne misbruges til konstruktion af målrettede angreb på systemet, hvilket vil udgøre en nærliggende risiko for kompromittering og potentiel misbrug af de store mængder persondata (billeder af pas og anden Billed-ID) i databasen. For DSB handler det således om at fastholde et højt niveau af kundernes/borgernes data i en situation, hvor DSB skal sikre dokumentation for, at alle rejsende har gyldig Billed-ID ved rejser til Sverige.

Da systemkompleksets 3 hovedelementer er sikkerhedsanalyseret separat, skal enkeltobservationer i de individuelle dokumenter ses i sammenhæng.

Grundet ovenstående ricisi er det alene nogle få betroede medarbejdere i DSB, der kender indholdet af sikkerhedsanalyserne.

DSB's IT sikkerhedsafdeling vil for at imødekomme Folketingets Ombudsmands ønske, gerne fremvise den relevante dokumentation på et møde. Derved vil Folketingets Ombudsmand kunne få præsenteret indholdet og få bekræftet, at DSB's standpunkt er velbegrundet og rimeligt. "

Jeg bad med brev af 21. marts 2016 om dine eventuelle bemærkninger til sagen.

Du anførte i en e-mail af 24. marts 2016 bl.a.:

"DSB har i sit afslag om aktindsigt henvist til offentlighedslovens § 23, stk. 1 (interne dokumenter). DSB har ligeledes undersøgt om § 26 (herunder nr. 3) samt §§ 28-29 (ekstraheringspligtige oplysninger) har fundet anvendelse, hvilket de ikke har efter DSB's opfattelse.

Min klage til først DSB, herefter Ombudsmanden gik på, at jeg var uenig i at offentlighedslovens § 26, nr. 3 ikke nødvendigvis fandt anvendelse – og jeg bad DSB redegøre hvorfor den ikke gjorde. Dette finder jeg stadig ikke svar på i nærværende udtalelse fra DSB.

Derimod oplyser DSB nu om nye beskyttelseshensyn. DSB argumenterer alene ud fra at oplysninger, ikke sagen eller akterne, skal undtages aktindsigt.

Jeg har forståelse for, at visse oplysninger i sikkerhedsanalyserne har en karakter, der kan berettige undtagelse fra aktindsigt. Dette kunne fx være efter offentlighedslovens § 30, nr. 2 eller § 33, nr. 3. Dog er jeg usikker på, om man her kan tale om en 'økonomisk interesse'.

Jeg vil dog mene, at givet den 'nærliggende risiko for kompromittering og potentiel misbrug af de store mængder persondata (billeder af pas og anden BilledID)', er det i offentlighedens interesse at kende til sikkerhedsanalysernes vurderinger og konklusioner.

I min oprindelige klage til DSB og Folketingets Ombudsmand, klagede jeg ikke over vurderingen i forhold til ekstraheringspligten. Såfremt det er muligt og relevant, beder jeg ombudsmanden vurdere, om der er ekstraheringspligtige oplysninger i sikkerhedsanalyserne, i det tilfælde at ombudsmanden mener sikkerhedsanalyserne ikke er omfattet af offentlighedslovens § 26, nr. 3. "

DSB meddelte den 8. april 2016, at DSB ikke havde bemærkninger til indholdet af din e-mail af 24. marts 2016. DSB skrev desuden følgende:

"Jeg skal i øvrigt orientere om, at DSB natten mellem mandag den 11. og tirsdag den 12. april 2016 stopper med at fotografere kundernes billed-id, når de passerer id-kontrollen på stationen ved Københavns Lufthavn. Alle rejsende til Sverige vil fortsat skulle vise gyldig billed-id for at passere id-kontrollen og tage toget til Sverige. Den nuværende kontrolprocedure opretholdes således på uændrede vilkår, blot uden fotografering.

Siden id-kontrollen blev indført den 4. januar 2016 har omkring en million rejsende passeret id-kontrollen. DSB har kun modtaget ganske få henvendelser fra den svenske politimyndighed om konkrete hændelser, og ultimo marts 2016 har DSB fra Transportstyrelsen i Sverige modtaget meddelelse om, at hændelserne frafaldes. På den baggrund har DSB vurderet, at processen for gennemførelse af id-kontrol,

som DSB har etableret, er effektiv og udgør et tilstrækkeligt dokumentationsgrundlag over for de svenske myndigheder. DSB har derfor besluttet at ophøre med at fotografere billed-id for at minimere generne for kunderne, så id-kontrollen kan ske hurtigere, når kunderne fremover skal med toget.

De billedfiler, som er lagret i DSB's ID-database, slettes samtidig med tidspunktet for ophør af fotografering.

Såfremt situationen ændrer sig, og de svenske myndigheder måtte vurdere, at DSB ikke kan dokumentere at DSB lever op til sit transportøransvar, vil DSB med kort varsel kunne genindføre fotograferingen af billed-id. "

Jeg sendte den 11. april 2016 en kopi af DSB's e-mail af 8. april 2016 til dig til orientering.

Den 30. maj 2016 havde to af mine medarbejdere et møde med DSB, hvor DSB forklarede nærmere om baggrunden for og sammensætningen af det system, som de omhandlede sikkerhedsanalyser vedrører. DSB fremviste desuden eksempler og uddrag fra rapporter vedrørende de gennemførte sikkerhedsanalyser.

DSB oplyste desuden, at rapporterne er udarbejdet af en virksomhed, som har særlig ekspertise i at gennemføre tests og sikkerhedsanalyser af IT-systemer, og at de herefter er sendt til DSB.