Charlotte Pedersen, director og Julie Suhr, consultant – Deloitte 3. juli 2012

Ny udtalelse[1] fra Datatilsynet tyder på en betinget anerkendelse af Microsofts cloud-løsning

I starten af juni kom Datatilsynet med en positiv ladet udtalelse omkring anvendelsen af cloud-leverandører. Betyder denne udtalelse, at danske organisationer og virksomheder nu trygt kan bruge cloud-løsninger også fra udenlandske leverandører?

Den nyeste udtalelse fra Datatilsynet om Microsofts behandling af personoplysninger i en cloud-løsning fra den 7. juni 2012 er mere positivt indstillet end den de offentliggjorde tilbage i 2011. Dengang handlede det om Odense kommune og deres ønske om at bruge Google Apps online. Microsofts løsning er anderledes på flere områder og synes også at imødekomme flere af de ankepunkter Datatilsynet havde mod Google.

En af de væsentligste årsager til at Odense kommunes Google-løsning ikke blev betragtet som tilstrækkelig i forhold til den danske lovgivning, var at den databehandleraftale, som man benyttede ikke overholdt Persondatalovens (PDLs) formelle krav. Databehandleraftalen var betinget af, at Google overholdt egne retningslinjer for it-sikkerhed, hvilket efter Datatilsynets opfattelse var en undermine-ring af PDLs formål om, at databehandler kun må handle på den dataansvarliges instrukser. Cloud leverandøren bør ikke gennem sine egne retningslinjer ensidigt kunne sætte betingelserne for aftalen mellem parterne (og dermed afvige fra aftalte instrukser).

Microsoft har efter sigende implementeret kommissionens standardkontrakt (model clause) for data-behandling, og danske dataansvarlige vil derfor have *muligheden* for at indgå en aftale med Microsoft om overførsel til tredjelande med de fornødne betingelser.

Delt ansvar?

Datatilsynet fremhæver dog, at de dataansvarlige stadig skal sikre sig, at standardbetingelserne rent faktisk inkluderes i aftalen, eftersom disse ikke automatisk medtages i Microsofts licensprocedure for alle kunder.

Som udgangspunkt er dette også den dataansvarliges opgave, men datatilsynet synes for første gang at nævne databehandlernes selvstændige ansvar for at sikkerhedsforanstaltningerne er på plads jfr. PDL § 41, stk. 3, 2. pkt.

---

[1] Link til Datatilsynets udtalelse om Microsofts cloud-løsning: http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/behandling-af-personoplysninger-i-cloud-loesningen-office-365/

Link til Persondataloven: https://www.retsinformation.dk/forms/r0710.aspx?id=828

De nævner således i udtalelsen at: *"Efter Datatilsynets opfattelse bør Microsoft give letforståelig information herom, før en kunde i Danmark indgår aftale om brug/køb af Office 365-ydelser. Kunden skal i den forbindelse have tydelig besked om, at kunden skal indgå en tredjelandskontrakt og databehandleraftale."*

I udtalelsen til Odense kommune nævner Datatilsynet slet ikke databehandlers ansvar, og det skyldes muligvis, at Datatilsynet netop havde fokus rettet mod den dataansvarliges forpligtelser, idet det netop var en dataansvarlig, der havde anmodet om selve udtalelsen. Den nyeste udtalelse henvender sig derimod mere til Microsoft som databehandler, og bærer præg af, at være en overordnet udtalelse mere end en konkret vurdering af den specifikke løsning.

Udmeldingen kan måske også ses som en indikation af, at Datatilsynet måske i højere grad end tidligere ser ansvaret som delt mellem den dataansvarlige og databehandleren? Hvis praksis på området går i denne retning, kan det potentielt gøre hele udfordringen omkring cloud computing mere håndgribelig.

En stor del af problemet omkring sikkerheden i cloud computing skyldes nemlig, at udbyderne af løsningerne ikke har haft incitamenterne til at overholde den danske sikkerhedsbekendtgørelse. De er ofte etableret i USA, og overholder derfor den amerikanske privacy lovgivning. Når ansvaret for EU-lovgivningen alene ligger hos den danske virksomhed/myndighed, har de store amerikanske cloud leverandører naturligt haft problemer med at finde interessen for de europæiske standarder.

De danske virksomheder og myndigheder, som ser store omkostningsfordele ved cloud løsningerne, har længe syntes at stå mellem 2 kedelige valg; enten at tage imod de betingelser de nu kunne få fra de amerikanske leverandører og dermed risikere sikkerhedshændelser og bøder og påtaler fra Datatilsynet, *eller* at vælge de gammeldags og dyrere løsninger, som overholder den danske lovgivning.

Hvis Datatilsynet begynder at tildele databehandlere et selvstændig ansvar i deres praksis og uddele sanktioner og udtalelser direkte til cloudleverandøren ved eventuelle overtrædelser, flyttes en del af de lovgivningsmæssige risici over på databehandlernes vægtskål,. Det vil sandsynligvis gøre cloud leverandørerne en del lettere at forhandle med, og de vil naturligvis have en større grund til, at optimere sikkerheden i deres løsninger.

Datatilsynet skal ikke godkende aftaler – det er den dataansvarliges opgave

En anden faktor som Datatilsynet fremhæver flere gange i den seneste udtalelse er, at de ikke skal godkende databehandleraftaler, men kun skal modtage skriftlige erklæringer om, at aftalen opfylder Kommissionens standardkontrakt. Det vil sige, at det er de dataansvarliges ansvar selv at vurdere, hvorvidt aftalen er i overensstemmelse med standardkontrakten eller ej.

Kun hvis den dataansvarlige konstaterer afvigelser fra standardkontrakten i selve databehandleraftalen eller i sideordnede aftaledokumenter, skal der indsendes en anmodning om godkendelse af disse afvigende vilkår, hvor databehandleraftalen indsendes som bilag.

Et af de elementer som de enkelte dataansvarlige selv skal vurdere, er hvorvidt kontrakten giver de fornødne forudsætninger for, at dataansvarlig kan kontrollere databehandlers faktiske sikkerhedsforanstaltninger. Dette er ikke en enkel opgave.
I Odense Kommune-sagen var Datatilsynet eksempelvis ikke tilfreds med, at man som dataansvarlig ikke kendte den nøjagtige placering af data, og det blev vurderet at muligheden for kontrol reelt set ikke var til stede.

Microsoft er tilsyneladende gået et lille skridt videre i forhold til Google, idet der i aftalen åbnes op for, at Datatilsynet efter skriftlig anmodning kan få tilsendt adresserne på datacentres placering. Datatilsynet er efter deres udtalelse at dømme tilsyneladende tilfreds med denne betingelse, selvom den dataansvarlige stadig ikke ligger inde med adresserne.

Ifølge Microsofts mundtlige udtalelse til Datatilsynet kan kunderne også under *visse omstændigheder* få lov til at inspicere et eller flere datacentre. Det er igen interessant, at Datatilsynet ikke stiller sig kritiske overfor sådan en betingelse, hvor de dataansvarlige altså ikke i alle tilfælde har muligheden for at inspicere forholdene, men kun under "visse" omstændigheder. Det er uklart om disse omstændigheder klart vil blive defineret i den enkelte aftale, men uanset hvad, vil det være den dataansvarliges ansvar at sikre sig dette, da Microsoft ikke vil være bundet af de udtalelser og formålserklæringer de måtte have forelagt Datatilsynet.

Datatilsynet har således vurderet, at muligheden for en lovlig aftale synes at være til stede i tilfældet med Microsoft. Der ligger nu et stort leverandørstyringsarbejde forude for de dataansvarlige.

Den dataansvarliges leverandørstyring
Den dataansvarlige efterlades med noget af en opgave, når det skal vurderes, om de aftaler der indgås er i tråd med sikkerhedsbekendtgørelsen og standardkontrakten eller ej.

En ting er, at leverandøren proklamerer at overholde standardkontrakten, men hvis databehandleraftalen eller sideordnede aftaledokumenter samtidig indeholder konkrete betingelser, der strider direkte imod selv samme standard, må man gå ud fra, at det stadig er den dataansvarlige, der har ansvaret for de konsekvenser, der måtte komme.

PDL og Sikkerhedsbekendtgørelsen stiller som bekendt en lang række andre krav. Der er f.eks. særlige krav til logning og kryptering, hvis der er tale om følsomme oplysninger, og den dataansvarlige skal

vurdere klassifikationen af data, og sikre de rette autorisationsprocedurer og efterleve reglerne for fysisk sikkerhed osv.

Så længe ansvaret for databehandlingen ligger på de dataansvarlige skuldre, vil det være nødvendigt at bruge en hel del ressourcer på leverandørstyring og kontroller.

Ikke alle dataansvarlige i Danmark har de tilstrækkelige faglige og økonomiske ressourcer til at gennemføre et sådan arbejde.

Markedet kunne muligvis være tjent med en mere ligelig fordeling af ansvaret mellem dataansvarlig og databehandler, så der blev større grobund for interessebaserede partnerskaber med lavere omkostninger pr. aftale.

Datatilsynet forventes snart at udkomme med en mere konkret udtalelse om IT-Universitetets anvendelse af Microsofts Office 365, og det skal blive spændende om den kaster mere lys over gældende ret på området – både hvad angår ansvarsfordelinger og de konkrete krav til aftalebetingelserne.