DANIEL LUNDQVIST OCH FREDRIK GUSTAFSSON

I EN NYLIGEN MEDDELAD dom slår Förvaltningsrätten i Stockholm fast att Salems kommuns användning av molntjänsten Google Apps kan innebära att personuppgifter behandlas på ett olagligt sätt. Om inte avtalsvillkoren för Google Apps ändras, så får kommunen inte längre använda molntjänsten. Avgörandet är det senaste i en rad beslut och domar som bekräftar att publika molntjänster fortfarande har svårt att uppfylla kraven i PUL.

Avtalsvillkor för molntjänster

▶ strider fortfarande mot PUL

Vi har flera gånger tidigare tagit upp molntjänster och de juridiska och säkerhetsmässiga krav som ställs på molntjänster utifrån bestämmelserna i personuppgiftslagen, PuL. Som bekant ökar användningen av molntjänster stadigt, såväl i privat som i offentlig sektor. Särskilt populärt är det att köpa programvara som molntjänst (software-as-a-service, SaaS), som exempelvis Google Apps, Dropbox eller Microsoft Office 365.

Inköp av molntjänster måste dock föregås av en noggrann analys av PuLs krav. Svårigheterna att förena PuL med molntjänstleverantörernas avtalsvillkor har framgått i en rad beslut från Datainspektionen, se till exempel beslut rörande Dropbox, Google Apps, Office 365 och Windows Azure (dnr 256-2011, 1351-2012, 1475-2013, 358-2014 och 574-2011).

Det är viktigt att påpeka att de juridiska frågeställningarna utifrån PuL är desamma, oavsett om kunden är en kommun, en myndighet eller ett privat bolag/organisation. Så länge molntjänsten medför att molntjänstleverantören automatiserat behandlar personuppgifter för vilka kunden är personuppgiftsansvarig så måste kraven i PuL beaktas.

DEN 1 JULI i år meddelade förvaltningsrätten dom angående Salems kommuns användning av Google Apps. Förvaltningsrätten gjorde samma bedömning som Datainspektionen tidigare gjort. Domstolen avslog därför kommunens överklagande. I korthet ansåg förvaltningsrätten att avtalet mellan kommunen och Google gav Google alltför stort utrymme att behandla de registrerades personuppgifter för sina egna ändamål, att en tillräckligt precis tid för lagring av personuppgifter saknades och att kommunen saknade tillräcklig information om vilka underleverantörer som Google anlitade för behandlingen. Detta betyder att Salems kommun inte får använda Google Apps under nuvarande avtal med Google.

Förvaltningsrättens dom har bäring även på andra publika molntjänster, vars avtalsvillkor sannolikt inte heller kan anses uppfylla PuL. Den här bilden bekräftas av flera nya granskningar och beslut från Datainspektionen.

I april 2014 granskade till exempel Datainspektionen Ale kommuns användning av Office 365 (dnr 1475-2013). Datainspektionen konstaterade att Ale kommuns avtal med Microsoft visserligen uppfyller många av PuLs krav men att det ändå finns brister utifrån kraven i PuL. Kritiken gällde framför allt att Ale kommun inte fick nödvändig och tillräcklig information om i vilka länder som Microsofts underleverantörer är lokaliserade och har sin verksamhet. I ett annat beslut från juni 2014 (dnr 358-2014) bedömdes Malmö stads användning av Google Apps for Education strida mot samma krav i PuL.

MOT BAKGRUND AV den senaste utvecklingen på området har vi tagit fram en enkel checklista med några av de viktigaste frågorna i PuL. De behöver övervägas inför ett beslut att börja använda molntjänster:

1. Krav på personuppgiftsbiträdesavtal
Det måste finnas ett skriftligt personuppgiftsbiträdesavtal mellan personuppgiftsansvarig (kunden) och personuppgiftsbiträdet (molntjänstleverantören). Det är viktigt att tänka på att kundens ansvar som personuppgiftsansvarig inte kan delegeras till molntjänstleverantören. Svensk lag måste tillämpas på avtalsförhållandet.

2. Ändamålet med behandling av personuppgifter
Personuppgifter får bara samlas in för uttryckligt angivna och berättigade ändamål. Insamlade personuppgifter får inte behandlas för något ändamål som är oförenligt med de ändamål som personuppgifterna ursprungligen samlades in för. Molntjänstleverantörer får därför inte behandla personuppgifter för egna ändamål, som inte instruerats av kunden. Enligt avtalet mellan Salems kommun och Google så tilläts Google till exempel att behandla personuppgifter i syfte att tillhandahålla eller underhålla sina system. Detta var enligt förvaltningsrätten inte förenligt med PuL, eftersom det gav Google viss möjlighet att bestämma ändamålen med behandlingen av kundens personuppgifter.

”PUL ställer långtgående krav på avtalsinnehåll och säkerhetsåtgärder för att en molntjänst ska anses uppfylla lagens krav...

3. Lagring av personuppgifter
Personuppgifter får inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det innebär bland annat att avtalet mellan kunden och molntjänstleverantören ska reglera att personuppgifterna ska raderas då avtalet upphör och inom skälig tid från det att kunden begär det. Det är enligt förvaltningsrätten inte tillräckligt att avtalet anger att personuppgifterna raderas inom viss tid, baserat på kommersiella hänsyn (”after a commercially reasonable time”), utan lagringstiden ska anges mer exakt. Lagringstiden kan dock vara förhållandevis lång. Datainspektionen har bland annat ansett att det är tillräckligt att personuppgifterna utplånas inom 180 dagar från det att de har markerats för radering (se dnr 1475-2013).

4. Insyn i vilka underleverantörer som används
Kunden måste ha kännedom om vilka underleverantörer till molntjänstleverantören som behandlar personuppgifter på uppdrag av molntjänstleverantören och i vilka länder de är lokaliserade. Det behövs bland annat för att kunna avgöra om landet har tillräcklig skyddsnivå. Enligt förvaltningsrätten är det inte tillräckligt att parterna har en muntlig överenskommelse, enligt vilken kunden kan få information om vilka underleverantörer som behandlar personuppgifter.

5. Avtal med underleverantörer
Avtal mellan molntjänstleverantören och dess underleverantörer ska återspegla avtalet mellan kunden och molntjänstleverantören. Det kan lösas genom att kunden ger molntjänstleverantören fullmakt att ingå avtal med underleverantörer på samma villkor som avtalet mellan kunden och molntjänstleverantören, samt att molntjänstleverantören för en förteckning över underleverantörer.

6. Säkerhet
Kunden ska vidta ”lämpliga tekniska och organisatoriska åtgärder” för att skydda de personuppgifter som behandlas. Kunden ska dessutom förvissa sig om att molntjänstleverantören kan genomföra de säkerhetsåtgärder som måste vidtas och att denne verkligen vidtar dessa. Detta kan bland annat säkerställas genom rätten till revision på plats hos molntjänst- och underleverantörer.

7. Risk- och sårbarhetsanalys
I de flesta fall ska kunden utföra en så kallad risk- och sårbarhetsanalys innan några personuppgifter behandlas i molnet. Närmare information om en sådan analys finns på Datainspektionens webbplats.

8. Överföring till - och behandling i - tredje land
Många molntjänstleverantörer använder infrastruktur eller resurser utanför EU/EES, vilket innebär att särskilda krav ställs enligt PuL. Det är upp till kunden att bedöma om överföringen och behandlingen av personuppgifter är förenlig med dessa krav. Frågan kan dock normalt lösas genom olika avtalskonstruktioner mellan kunden och molntjänstleverantören.

9. Instruktioner till anställda m m
Kunden ska ge tydliga instruktioner till sina anställda med flera, så att det tydligt framgår om och under vilka förutsättningar de som arbetar under kundens ledning får behandla personuppgifter i en molntjänst.

SAMMANFATTNINGSVIS STÄLLER PuL långtgående krav på avtalsinnehåll och säkerhetsåtgärder för att en molntjänst ska anses uppfylla lagens krav. Samtidigt har många av de ledande leverantörerna av publika molntjänster fortfarande svårt att uppfylla kraven, ofta på grund av tjänsternas globala uppbyggnad och höga standardiseringsgrad.

För företag som vill använda molntjänster innebär detta att omfattande resurser måste tillsättas (eller anlitas) för att verifiera leverantörens lösning och avtalsvillkor. Efter den senaste framgången i förvaltningsrätten kommer Datainspektionen säkert att fortsätta driva rättsutvecklingen, vilket vi följer med spänning! ●

DANIEL LUNDQVIST
är advokat och arbetar i Advokatfirman Delphis TMT-grupp. Daniel biträder svenska och internationella klienter i frågor om IT-rätt, integritetsskydd, outsourcing och kommersiell avtalsrätt.

FREDRIK GUSTAFSSON
är jur.kand. och biträdande jurist i Delphis TMT/Intellectual Property-grupp. Fredrik arbetar huvudsakligen med IT-avtal och immaterialrättsliga ärenden, med särskilt fokus mot integritetsskyddsaspekter.