

2017-08-07

TJÄNSTESKRIVELSE
KFKS 2017/692

Kommunstyrelsen

Informationssäkerhet vid outsourcing

Förslag till beslut

Kommunstyrelsen noterar informationen om hur kommunen hanterar informationssäkerhet vid outsourcing.

Sammanfattning

Med anledning av diskussionen om informationssäkerhet vid outsourcing beskrivs i ärendet hur kommunen hanterar denna fråga. Kommunen har ingen egen drift av IT-system. I de fall kommunen skulle kunna haft det har driften av tjänsterna outsourcats. Kommunen har krävställt att driften ska ske i Sverige med personal anställd i Sverige. En del system köps som tjänst där ägaren av system även sköter om driften. Ett av de större system är det som används inom det sociala området. Även här sker driften i Sverige med personal anställd i landet. Oavsett om man outsorcar driften eller köper system som tjänst ska det finnas personuppgiftsbiträdesavtal. Kommunen har sådana avtal med leverantörer i de fall personuppgifter hanteras. Vidare sker i ett kontinuerligt arbete med att utveckla informationssäkerheten och höja kunskapen inom området.

Ärendet

Under sommaren har frågan om informationssäkerhet vid outsourcing av IT diskuterats en hel del. Med anledning av detta vill stadsledningskontoret förtydliga hur kommunen hanterar frågorna om informationssäkerhet vid outsourcing.

Kopplat till händelserna på Transportstyrelsen måste man vara klar över att det finns två lagar som styr hanteringen av information. Det är säkerhetsskyddslagen och personuppgiftslagen. Det lagbrott som gjorts på Transportstyrelsen är kopplat till säkerhetsskyddslagen och den styr ännu hårdare just vem som får hantera data och var det får lagras. I kommunen

hanterar vi ytterst lite data kopplat till säkerhetsskyddslagen (då det oftast är kopplat till rikets säkerhet) men vi har stora mängder data som lyder under personuppgiftslagen. Information som omfattas av denna lag får lagras inom EU och hanteras av personal som inte är svenska medborgare, men de ska då lyda under ett personuppgiftsbiträdesavtal.

Kommunen har sedan 2010 ingen egen organisation för drift av IT-system. De system som kommunen använder köps antingen som tjänst eller att driften av system görs av kommunens upphandlade leverantör. När man köper ett system som tjänst så ansvarar företaget som tillhandahåller systemet både driften av det och support och utveckling av själva systemet. I det andra fallet sköts driften av själva system av en leverantör medan företaget som äger systemet ansvarar för support och utveckling. Det är i det senare fallet som man kan välja att ha drift av system i egen regi.

Kommunen har beslutat att ha som strategi att inte ha drift i egen regi. Inför den andra upphandlingen av IT-drift tog kommunstyrelsen den 11 januari 2016 beslut om att dela upp det tidigare avtalet i fyra delar (sk multisourcing) med specialiserade företag för respektive del. Avsikten detta vara att få avtal med de som är bäst inom sitt område till bästa pris.

I september samma år var upphandlingarna klara och avtal slöts för drift med Basefarm. Basefarm är ett norskt företag med ett svenskt dotterbolag som har stor verksamhet i Sverige. I kravställningen hade kommunen begärt att serverdriften skulle utföras i Sverige, helst geografiskt nära kommunen. Så är också fallet idag. Kommunen använder två av Basefarms serverhallar, båda lokaliserade i Stockholm. Driften sköts av Basefarms personal anställda i Sverige och hanteringen av informationen är reglerat i ett personuppgiftsbiträdesavtal, utformat av kommunens juridik- och kanslienhet i enlighet med gällande lag.

Kommunen har upphandlat en särskild leverantör för tjänster kopplade till informationssäkerhet. Kommunen har avtal med ett av landets mest välrenommerade IT-säkerhetsföretag, Certezza. Designen av kommuns driftsmiljö är framtagen i samverkan med Basefarm och Certezza. Driften av systemen finns i flera säkerhetszoner där systemen placeras efter informationens säkerhetsklassningsnivå. Kommunen har på detta sätt en miljö som säkerhetsmässigt är av mycket hög och god klass. Det kan noteras att Basefarm även ansvarar för driften av Ineras system, bland annat 1177 vilket är ett av Sveriges system med högst säkerhetsklassning gällande personuppgifter.

Ett av de större system som kommunen köper som tjänst är Combine som används inom det sociala området. Det finns personuppgiftsbiträdesavtal och att driften sköts av Pulsen i Borås med säkerhetsklassad personal anställd av Pulsen.

Kommunen driver sedan ett kontinuerligt och långsiktigt arbete med att höja kunskapen och medvetenheten om informationssäkerhet. Det är inte minst viktigt kopplat till det nya dataskyddsdirektivet inom EU som träder i kraft i den 25 maj nästa år. I arbetet ingår att säkerställa att kommunens verksamheter har system med korrekta avtal och att informationen



är klassad på rätt sätt. Vidare ingår även utbildningsinsatser då den största risken alltid är den egna personalens hantering av riskklassat data.

Ekonomiska konsekvenser

Kostnader för system kopplat till informationssäkerhet, avtal med leverantörer och kompetensutveckling hanteras inom beslutad budget.

Konsekvenser för barn

Att information hanteras på ett säkert sätt är lika viktigt för alla, barn som vuxna.

Mats Bohman
Administrativ direktör
Stadsledningskontoret