

Enköpings kommunstyrelse
Kungsgatan 42
745 80 Enköping

Tillsyn enligt personuppgiftslagen (1998:204) – Enköpings kommunstyrelsens användning av molntjänsten Dropbox

Datainspektionens beslut

- Datainspektionen konstaterar följande:
 1. Kommunstyrelsen är personuppgiftsansvarig för den personuppgiftsbehandling som deras anställda utför i tjänsten.
 2. I egenskap av personuppgiftsansvarig har kommunstyrelsen det fulla ansvaret för att behandlingen av personuppgifter utförs i enlighet med dataskyddsbestämmelserna i svensk lag. Detta förändras inte av att personuppgiftsbehandlingen utförs av personuppgiftsbiträden.
 3. Datainspektionen konstaterar att både Dropbox Inc. och dess underleverantörer, som behandlar personuppgifter för kommunstyrelsens räkning, är personuppgiftsbiträden till kommunstyrelsen.

- Datainspektionen förelägger kommunstyrelsen att ge tydliga instruktioner till dem som arbetar under kommunstyrelsens ledning så att det blir tydligt om, och i så fall under vilka förutsättningar, kommunstyrelsen tillåter lagring av arbetsmaterial och annat material som innehåller personuppgifter i Dropbox.

- Datainspektionen förutsätter därvid att kommunstyrelsen gör en bedömning av om kommunanställdas användning av Dropbox i tjänsten – för behandling av personuppgifter på andra sätt än genom lagring av dokument som lagligen publicerats på Internet – är tillåten enligt personuppgiftslagen. Datainspektionen förutsätter vidare att kommunstyrelsen genomför en risk- och sårbarhetsanalys av behandlingen.

Datainspektionen kan komma att följa upp beslutet.

Redogörelse för tillsynsärendet

Bakgrund

I januari 2011 påbörjade Datainspektionen ett tillsynsprojekt för att undersöka olika personuppgiftsansvarigas användning av molntjänster. Syftet med projektet är att kontrollera om personuppgiftslagens bestämmelser följs då molntjänster används för att behandla personuppgifter och att sprida kunskap om personuppgiftslagen och dess krav. I projektet har tre inspektioner genomförts, däribland en inspektion av Enköpings kommunstyrelses (fortsättningsvis kommunstyrelsen) användning av Dropbox.

Datainspektionen tar i det här beslutet inte ställning till huruvida molntjänstanvändningen är förenlig med andra bestämmelser än de i personuppgiftslagen, till exempel offentlighets- och sekretesslagen (2009:400).

Inspektionen av kommunstyrelsen genomfördes den 18 mars 2011. Protokoll över inspektionen har upprättats och översänts till kommunstyrelsen. Kommunstyrelsen har yttrat sig över protokollet och har i samband med det också svarat på Datainspektionens kompletterande frågor. I ärendet har bl.a. följande framkommit.

Användning av Dropbox för distribution av kallelser, handlingar och protokoll
Kommunstyrelsen använder en gratisversion av Dropbox för att förmedla kallelser, handlingar och protokoll till tjänstemän samt ledamöter i kommunstyrelsen och arbetsutskotten inför nämndsammanträden. Det är 22 personer som använder Dropbox för detta ändamål. Samma handlingar som delas ut genom Dropbox publiceras även på kommunens webbsida. Kommunstyrelsen har uppgett att deras avsikt är att varje dokument ska granskas och bedömas enligt 12 § personuppgiftsförordningen, vilket innebär exempelvis att personnummer inte ska publiceras på webbsidan eller i Dropbox. Om det bedöms att dokumenten inte kan publiceras på webbsidan distribueras dessa på annat sätt än genom Dropbox. Uppläggningsen av dokument i Dropbox görs antingen av kanslijuristen, som är sekreterare i nämnden, eller av en assistent på kansliet, i samråd med kanslichefen. Kommunstyrelsen har uppgett att det är ovanligt att det förekommer personuppgifter i de aktuella handlingarna. Ärenden som kan förekomma är beslut om inriktning, policyfrågor samt svar på motioner. Det finns ingen koppling mellan ärendehanteringssystemet och Dropbox.

Övrig användning av Dropbox

Vid inspektionen har också framkommit att det inte finns något som hindrar anställda och andra från att använda Dropbox för att spara och dela andra dokument än de som kommunstyrelsen avsett. Kommunstyrelsen har varken uppmuntrat eller avrått från sådan användning. Vidare har det framkommit att kommunstyrelsen har kännedom om att det är en handfull inom kommunstyrelsen som använder Dropbox i tjänsten, i stället för USB-minnen, för att spara olika typer av arbetsmaterial. Därutöver har också IT-enheten använt Dropbox för lagring av dokument under ett projekt. Projektdokumenterna ligger kvar i Dropbox. Kommunstyrelsen har uppgett att de utgår ifrån att de som använder Dropbox hanterar information som omfattas av sekretess på rätt sätt.

IT-säkerhet

Varje enskild användare av Dropbox har ett eget Dropbox-konto som denne själv skapat. Dokument i Dropbox går att komma åt via Dropboxes webbsida eller genom en Dropboxklient som installeras på datorn. På de datorer som tillhandahålls av kommunen kan endast de som har administrationsrättigheter installera Dropboxklienten.

Kommunstyrelsen sparar dokumenten som läggs upp i Dropbox i särskilda mappar för varje nämndmöte. Kommunstyrelsen har i användarlistan i Dropbox skapat grupper av de användare som ska få del av kallelser, handlingar och protokoll. De personer som ansvarar för att lägga upp dokument i Dropbox ansvarar också för att dela dokumenten med personerna i dessa grupper och för att plocka bort användare ur listan. Den som har fått åtkomst till en mapp i Dropbox kan i sin tur bjuda in andra till den mappen. Detta syns då i loggen "Events" och i användarlistan som kommunstyrelsen kan se i Dropbox.

Det sker ingen kryptering av uppgifter innan dessa läggs in i Dropbox. Kommunstyrelsen litar på den information som Dropbox ger på sin webbsida där det framgår att anställda hos Dropbox inte tar del av användarnas filer.

Dropbox Inc. (Dropbox) är kommunstyrelsens personuppgiftsbiträde. Vid inspektionen framkom att kommunstyrelsen inte har något personuppgiftsbiträdesavtal med Dropbox och att den inte kände till om Dropbox använde sig av några underleverantörer.

Skäl för beslutet

Personuppgiftslagen och användningen av molntjänster

Dagens dataskyddslagstiftning är i vissa avseenden svår att förena med det som vi idag kallar för molntjänster. Personuppgiftslagen, och dataskyddsdirektivet som lagen bygger på, utgår från att det är den personuppgiftsansvarige som är den starka, bestämmande aktören som faktiskt kan instruera och kontrollera vad dennes personuppgiftsbiträden gör. Den i ärendet granskade molntjänstanvändningen visar att verkligheten ser annorlunda ut. Det är personuppgiftsbiträdet som erbjuder en tjänst och som i standardavtal och policies anger vad som gäller vid tillhandahållande av tjänsten.

Möjligheterna för den personuppgiftsansvarige att formulera egna instruktioner och precisera vilka säkerhetsåtgärder som bör vidtas tycks ytterst begränsade. Istället för att formulera egna instruktioner och villkor för personuppgiftsbehandlingen måste den personuppgiftsansvarige granska de avtalsvillkor och riktlinjer som molntjänstleverantören erbjuder. Utifrån dessa måste den personuppgiftsansvarige kunna bedöma om den personuppgiftsbehandling som den personuppgiftsansvarige vill låta molntjänstleverantören utföra kommer att vara tillåten och tillräckligt säker. Den bedömningen måste göras med beaktande av personuppgiftslagens bestämmelser, om bl.a. ändamålen med behandlingen, tredjelandsoverföring och säkerhetsåtgärder samt slutsatserna av den personuppgiftsansvariges egen risk- och sårbarhetsanalys. Otydliga avtal och skrivningar som möjliggör för molnleverantören att ensidigt förändra villkoren för behandlingen medför stora risker eftersom den personuppgiftsansvarige då inte kan veta om den, genom anlitaandet av molntjänstleverantören, uppfyller personuppgiftslagens krav. Möjligheterna för den personuppgiftsansvarige att kontrollera behandlingen försvåras också när molntjänstleverantören låter flera juridiska personer, som också kan finnas i flera olika länder, behandla personuppgifterna.

Vid anlitaande av personuppgiftsbiträden finns det även annan lagstiftning än personuppgiftslagen som blir relevant vid olika former av uppgiftsutlämnanden. Datainspektionen konstaterar att många uppgifter hos t.ex. socialtjänsten omgärdas av stark sekretess och påminner därför om att den personuppgiftsansvarige givetvis måste beakta all relevant lagstiftning.

Personuppgiftsansvar

Enligt 3 § personuppgiftslagen är den personuppgiftsansvarige den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Vidare är, enligt samma bestämmelse, den som behandlar personuppgifter för den personuppgiftsansvariges räkning personuppgiftsbiträde. Ett personuppgiftsbiträde finns alltid utanför

den egna organisationen. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar är inte personuppgiftsbiträde.

Datainspektionen kan konstatera att det hos kommunstyrelsen förekommer användning av Dropbox utöver det tilltänkta tillhandahållandet av kallelser, handlingar och protokoll, samt att kommunstyrelsen är medveten om detta. Kommunstyrelsen har varken uppmuntrat eller avrått från sådan ytterligare användning. Datainspektionen konstaterar att kommunstyrelsen är personuppgiftsansvarig för den personuppgiftsbehandling som deras anställda utför i tjänsten.

Vidare konstaterar Datainspektionen att kommunstyrelsen i egenskap av personuppgiftsansvarig har det fulla ansvaret för att behandlingen av personuppgifter utförs i enlighet med dataskyddsbestämmelserna i svensk lag. Detta förändras inte av att personuppgiftsbehandlingen utförs av personuppgiftsbiträden.

Datainspektionen konstaterar också att både Dropbox och Dropboxes underleverantörer som behandlar personuppgifter för kommunstyrelsens räkning är personuppgiftsbiträden till kommunstyrelsen.

Tillämpliga bestämmelser

Personuppgiftslagen bygger på två regelsystem: hanteringsreglerna och missbruksregeln. Det är materialets struktur som avgör vilket regelsystem som blir tillämpligt. Av 5 a § personuppgiftslagen framgår att de allra flesta bestämmelserna i lagen (hanteringsreglerna) inte behöver tillämpas på behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. För sådan behandling gäller istället endast att den inte får utföras om den innebär en kränkning av den registrades personliga integritet (missbruksregeln).

Kommunstyrelsen har uppgett att det inte finns någon koppling mellan ärendehanteringssystemet och Dropbox. Mot bakgrund av detta bedömer Datainspektionen att kommunstyrelsens användning av Dropbox för tillhandahållande av kallelser, handlingar och protokoll innebär en behandling av personuppgifter i ett ostrukturerat material, vilket gör att missbruksregeln blir tillämplig.

För att avgöra om en behandling av personuppgifter är kränkande måste man göra en samlad bedömning av hur känsliga personuppgifterna är, i vilket sammanhang de förekommer, för vilket syfte de behandlas, vilken spridning

de har fått eller riskerar att få samt vad behandlingen kan leda till. I detta fall kan 12 § personuppgiftsförordningen ge vägledning vid kränkingsbedömningen (se Datainspektionens beslut, dnr 987-2009).

Datainspektionen utesluter inte att hanteringsreglerna skulle kunna bli tillämpliga vid annan användning av Dropbox. Kommunstyrelsen måste själv bedöma vilka regler som blir tillämpliga vid en viss behandling och se till att följa dessa.

Allmänt om personuppgiftslagens krav på säkerhet

Personuppgiftslagens säkerhetsbestämmelser i 30 -32 §§ ska tillämpas oavsett om det är hanteringsreglerna eller missbruksregeln som reglerar en behandling. Enligt 31 § första stycket personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Med organisatoriska åtgärder avses säkerhetsarbetets organisation och rutiner, instruktioner och policyer. Ju känsligare personuppgifter som behandlas, desto högre blir kraven på säkerhetsåtgärderna. Åtgärderna ska nämligen åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

Den säkerhetsnivå som bedöms tillräcklig för en viss personuppgiftsbehandling måste givetvis upprätthållas i alla lägen – även om den personuppgiftsansvarige anlitar någon annan för att utföra personuppgiftsbehandlingen åt sig. För att integritetsskyddet inte ska försämrats om den personuppgiftssansvarige anlitar någon annan måste, enligt 31 § andra stycket, den som anlitat ett personuppgiftsbiträde för behandling av personuppgifter förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

För att integritetsskyddet ska upprätthållas krävs också, enligt 30 § andra stycket personuppgiftslagen, att den personuppgiftsansvarige måste ha ingått ett skriftligt avtal med personuppgiftsbiträdet, i vilket det framgår att personuppgiftsbiträdet bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 31 § första stycket.

Av 30 § 1 stycket personuppgiftslagen framgår att ett personuppgiftsbiträde och de personer som arbetar under den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige.

Av förarbetena till bestämmelsen i 5 a § framgår att man, vid bedömningen av vilka åtgärder som behöver vidtas för att åstadkomma en lämplig säkerhetsnivå, kan ta hänsyn till bl.a. de risker som är förknippade med behandlingen. När personuppgifter behandlas i ostrukturerat material t.ex. i form av löpande text och ljud- och bildupptagningar torde det därför normalt inte krävas några extraordinära säkerhetsåtgärder utan det kan ofta räcka med de åtgärder som var och en brukar vidta för att skydda sin information. När särskilt känslig information behandlas i strukturerat eller ostrukturerat material måste givetvis adekvata säkerhetsåtgärder vidtas (prop. 2005/06: 173, s. 36).

Användning av Dropbox för distribution av kallelser, handlingar och protokoll
Datainspektionen har inget att invända mot kommunstyrelsens användning av Dropbox för distribution av kallelser, handlingar och protokoll. Det gäller under förutsättning att de personuppgifter som läggs upp på Dropbox ingår i samma dokument som publiceras på kommunens webbplats efter en bedömning utifrån gällande sekretessbestämmelser, 5 a § personuppgiftslagen och 12 § personuppgiftsförordningen. Eventuella säkerhetsbrister hos Dropbox bör rimligen inte medföra nämnvärda integritetsrisker för den enskilde, eftersom publiceringen av dokumenten på Internet får förutsättas vara laglig samt innebär att personuppgifterna finns allmänt tillgängliga. Vid en sådan behandling, som publicering på Internet innebär, tillför personuppgiftsbiträdesavtal inget mervärde för integritetsskyddet och Datainspektionen lämnar därför inga påpekanden gällande personuppgiftsbiträdesavtal i denna del.

Övrig användning av Dropbox

Datainspektionen har ovan konstaterat att kommunstyrelsen är medveten om att det förekommer att Dropbox används för t.ex. lagring av olika typer av arbetsmaterial, samt att kommunstyrelsen varken har uppmuntrat till eller avrått från sådan övrig användning. Datainspektionen kan också konstatera att kommunstyrelsen inte har kännedom om omfattningen eller känsligheten hos personuppgifterna som behandlas vid sådan användning, samt att kommunstyrelsen inte har vidtagit någon risk- och sårbarhetsanalys i detta avseende. Vidare kan Datainspektionen konstatera att kommunstyrelsen vid inspektionstillfället varken hade kännedom om att Dropbox anlitar underleverantörer eller hur avtalen, som de individuella användarna ingår med Dropbox, ser ut.

Enligt personuppgiftslagen 30 § 1 stycket får de personer som arbetar under den personuppgiftsansvariges ledning bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Datainspektionen anser att det i alla organisationer bör upprättas rutiner och instruktioner som beaktar personuppgiftslagens bestämmelser. Det är viktigt att anställda informeras om vad som är tillåtet, vilka konsekvenserna blir om man bryter mot

en regel och hur efterlevnaden av reglerna följs upp. Det har i ärendet inte framkommit att kommunstyrelsen har instruktioner som omfattar de anställdas användning av Dropbox. Datainspektionen förelägger därför kommunstyrelsen att ge tydliga instruktioner till dem som arbetar under kommunstyrelsens ledning så att det blir tydligt om, och i så fall under vilka förutsättningar, kommunstyrelsen tillåter lagring av arbetsmaterial och annat material som innehåller personuppgifter i Dropbox.

Framtagandet av instruktionerna måste föregås av att kommunstyrelsen gör en bedömning av om sådan användning av Dropbox är tillåten enligt personuppgiftslagen. Kommunstyrelsen måste granska de avtalsvillkor som Dropbox erbjuder och göra bedömningarna utifrån dessa. Bedömningen måste göras med beaktande av personuppgiftslagens bestämmelser och slutsatserna av den personuppgiftsansvariges egen risk- och sårbarhetsanalys. Den personuppgiftsansvarige måste bl.a. ta ställning till om det finns risk för att personuppgifter kan komma att behandlas för andra ändamål än de som den personuppgiftsansvarige får behandla personuppgifterna för. Vidare måste den personuppgiftsansvarige ha klart för sig om molntjänstleverantören kan komma att lämna över personuppgifter till ett s.k. tredjeland, dvs. ett land utanför EU/EES, och om den överföringen i så fall har stöd i personuppgiftslagen. Den personuppgiftsansvarige måste även ta ställning till vilka säkerhetsåtgärder som måste vidtas för att skydda de personuppgifter som behandlas och beakta kravet på att ett personuppgiftsbiträdesavtal ska upprättas med personuppgiftsbiträden. Även annan lagstiftning, t.ex. sekretesslagstiftning måste beaktas.

Kommunstyrelsen förutsätts därför också genomföra en risk- och sårbarhetsanalys av den övriga användningen av Dropbox. Risk- och sårbarhetsanalysen ska ligga till grund för bedömningen av vilken säkerhetsnivå som är lämplig för de personuppgifter som behandlas, vilka åtgärder som måste vidtas och om det är möjligt att anlita Dropbox för behandling av de tänkta personuppgifterna. Ju större integritetsrisker en viss personuppgiftsbehandling innebär desto högre är kraven på säkerhetsåtgärder. Hur stora integritetsrisker som en viss behandling innebär beror bland annat på antalet personer som de behandlade personuppgifterna avser, mängden personuppgifter som behandlas om varje person och känsligheten hos de behandlade personuppgifterna. Även möjligheten att strukturera personuppgifterna har i det här sammanhanget betydelse. Åtgärder bör övervägas när det gäller bl.a. autentisering, behörighetsstyrning, behörighetskontroll, kommunikationssäkerhet, rutiner för säkerhetskopiering och utplåning samt skydd mot obehörig trafik och skadlig programvara.

Det finns flera etablerade metoder för risk- och sårbarhetsanalys, t.ex. användandet av checklistor. Nackdelen med att använda en checklista är att den inte alltid är helt anpassad för den molntjänst man tänkt använda och att det finns risk för att man arbetar mekaniskt efter listan och därmed låter bli att tänka själv samt att verkligen analysera resultaten. En checklista för molntjänster har tagits fram av EU:s nätverks- och informationssäkerhetsbyrå ENISA; *Cloud Computing, Information Assurance Framework*.

För bedömningen av hur kommunstyrelsen ska kunna leva upp till kraven på skriftligt personuppgiftsbiträdesavtal i personuppgiftslagen 30 § andra stycket, kan kommunstyrelsen söka ledning i Datainspektionens beslut, dnr 263-2011.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde måste den, enligt personuppgiftslagen 31 § andra stycket, förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna. När det är fråga om s.k. molntjänster kan det på grund av den teknik som används vara svårt att svara på var uppgifter lagras eller bearbetas rent fysiskt och därmed även geografiskt. Om en molnleverantör utan användarens vetskap kan flytta uppgifter inte bara mellan olika underleverantörer men också mellan olika länder, minskar den personuppgiftsansvariges möjligheter att följa upp och försäkra sig om att personuppgiftsbiträden verkligen vidtagit de åtgärder de åtagit sig. En grundläggande förutsättning för att kunna uppfylla säkerhetskraven i 31 § personuppgiftslagen och kravet på kontroll av personuppgiftsbiträden är att den personuppgiftsansvarige har kännedom om vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning.

En förutsättning för att kommunstyrelsen ska kunna uppfylla kraven på kontroll av dem som behandlar personuppgifter för deras räkning är att kommunstyrelsen vet vilka de är skyldiga att kontrollera. Det gäller oavsett hur kommunstyrelsen väljer att uppfylla kraven på kontroll.

Datainspektionen kan komma att följa upp beslutet.

Hur man överklagar

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet skall ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder över-

klagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, teamledaren Catharina Fernquist, IT-säkerhetsspecialisten Adolf Slama samt juristerna Ulrika Andersson, Ulrika Harnesk och Lena Carlsson, föredragande.

Göran Gräslund

Lena Carlsson