Datainspektionen

Datum	Diarienr
2011-09-28	263-2011

Salems Kommunstyrelse
144 80 Rönninge

Tillsyn enligt personuppgiftslagen (1998:204) – Salems kommunstyrelse

Följande beslut avser Salems kommunstyrelses (fortsättningsvis kommunstyrelsen) användning av Google Apps tjänster e-post, kalender och chat samt i ett avseende kommunstyrelsens planerade användning.

Datainspektionens beslut

- Datainspektionen konstaterar följande:
  1. I egenskap av personuppgiftsansvarig har kommunstyrelsen det fulla ansvaret för att den behandling av personuppgifter som sker genom användandet av Google Apps utförs i enlighet med dataskyddsbestämmelserna i svensk lag. Detta förändras inte av att personuppgiftsbehandlingen utförs av ett personuppgiftsbiträde.
  2. Samtliga bolag inom Googlekoncernen som behandlar eller kan komma att behandla personuppgifter för kommunstyrelsens räkning är personuppgiftsbiträden till kommunstyrelsen.
  3. Den behandling som kommunstyrelsen utför för administration och kontroll av e-post, kalender och chat har sådan personuppgiftsanknuten struktur att hanteringsreglerna i PuL gäller.
  4. Ingivna avtal mellan kommunstyrelsen och Google lever inte upp till kraven på personuppgiftsbiträdesavtal i 30 § andra stycket personuppgiftslagen.
  5. Kommunstyrelsen lever inte upp till kraven i 31 § andra stycket personuppgiftslagen, eftersom kommunstyrelsen inte har kunskap om vilka bolag inom personuppgiftsbiträdets koncern som behandlar personuppgifter för dennes räkning.

- Datainspektionen förelägger kommunstyrelsen att upprätta personuppgiftsbiträdesavtal som lever upp till kraven i personuppgiftslagen.

  Personuppgiftsbiträdesavtal upprättas antingen genom tecknande av ett

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

avtal med varje bolag inom Googlekoncernen, som behandlar personuppgifter för kommunstyrelsens räkning, eller genom att i ett avtal ge Google Ireland Ltd eller Google Inc mandat att ingå ett avtal med underbiträden, där det förskrivs att varje personuppgiftsbiträde har samma skyldigheter som det personuppgiftsbiträde som kommunstyrelsen själv ingått avtal med.

Villkoren i personuppgiftsbiträdesavtalet ska vara urskiljbara från övriga villkor som gäller mellan parterna. Personuppgiftsbiträdesavtalets villkor ska inte ensidigt kunna förändras av personuppgiftsbiträdet och följande ska finnas reglerat. Personuppgiftsbiträdesavtalet ska

1. föreskriva att personuppgiftsbiträdet är skyldigt att tillämpa svensk lagstiftning när det gäller behandlingen av personuppgifter,
2. föreskriva att personuppgiftsbiträdet är skyldigt att vidta lämpliga säkerhetsåtgärder enligt 31 § personuppgiftslagen,
3. föreskriva att Googleföretagen endast får behandla personuppgifter i enlighet med kommunstyrelsens instruktioner och därmed säkerställa att personuppgiftsbiträdet inte behandlar personuppgifter för andra ändamål än dem som kommunstyrelsen anlitat personuppgiftsbiträdet för,
4. säkerställa att kommunstyrelsen har kännedom om vilka personuppgiftsbiträden som kan komma att behandla kommunens personuppgifter,
5. säkerställa att kommunstyrelsen på lämpligt sätt har möjlighet att följa upp att personuppgiftsbiträden lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen vidtar lämpliga säkerhetsåtgärder,
6. säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstanke om obehörig åtkomst av personuppgifter inom kommunen eller hos Googleföretagen,
7. säkerställa att parterna vet vilka åtgärder som ska vidtas vid avtalets upphörande så att personuppgiftsbiträdet inte längre har åtkomst till personuppgifterna därefter.

- Datainspektionen förlägger vidare kommunstyrelsen att förvissa sig om att alla bolag som behandlar kommunstyrelsens personuppgifter i tredje land har anslutit sig till Safe Harbor-principerna eller att överföringen är tillåten på någon annan grund.

- Datainspektionen erinrar kommunstyrelsen om att den måste se över sin e-postpolicy och tydligt instruera sina medarbetare om vilka personuppgifter som inte får skickas med e-post utan att de först krypteras.

- Datainspektionen erinrar kommunstyrelsen om att den måste genomföra en risk- och sårbarhetsanalys gällande personuppgiftsbehandling för kommunstyrelsens framtida användning av molntjänster.

Datainspektionen avser att följa upp beslutet.

Redogörelse för tillsynsärendet

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 kommunstyrelsen.

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 25 mars 2011. Protokoll över inspektionen har upprättats och översänts till kommunstyrelsen. Kommunstyrelsen har inkommit med svar på kompletterande frågor samt med yttrande över protokollet.

Tillsynsbeslutet riktar sig endast mot kommunstyrelsen och Datainspektionens granskning har utgått från den användning av Google Apps som testades vid inspektionstillfället – tjänsterna e-post, kalender och chat. I ärendet benämns kommunstyrelsens användning av tjänsterna e-post, kalender och chat som *den aktuella användningen*. Tillsynsbeslutet omfattar inte övriga kommunala nämnders personuppgiftsbehandling. I ärendet har också framkommit att Salems kommun (kommunen) som helhet avser att använda sig av ytterligare tjänster i Google Apps, utöver tjänsterna e-post, kalender och chat. Datainspektionen benämner fortsättningsvis den användningen som *den planerade användningen*.

Aktuell användning och planerad användning

Kommunen hade vid inspektionstillfället tecknat avtal att börja använda Google Apps för anställda och elever. Vid inspektionstillfället hade användningen inte startat. Vid tidpunkten för inspektionen körde IT-enheten (åtta personer) en pilot av e-post, chatt och kalender. I telefonsamtal den 18 maj 2011 har kommunstyrelsen bekräftat att användningen av Google Apps användning av e-post, kalender och chat är i gång. Vidare avsåg kommunstyrelsen samt kommunen i övrigt att börja använda funktionerna Google Presentation den 1

juli 2011 och Google Docs, kalkyl och text den 1 september 2011. De IT-verktyg som socialtjänst, vård och skola använder sig av ska läggas ut sist, senast 2015. Socialtjänsten har idag egna ordbehandlingsprogram.

Kommunstyrelsens avtalsparter och ingångna avtal

Kommunen har genom en återförsäljare tecknat avtal med Google Inc om användning av Google Apps Premier Edition (för anställda) och Google Apps Education Edition (för eleverna). Avtalen är i grunden desamma men innehåller olika hänvisningar. Avalon Information Systems AB är återförsäljare och behandlar inga personuppgifter för kommunens räkning.

Google Inc har, efter att avtal tecknats, överlämnat till Google Ireland Ltd att ingå avtal med kommunstyrelsen vilket gjorts i tilläggsavtal. Kommunstyrelsen har uppgivit att det är Google Irland Ltd som är ansvarigt gentemot kommunstyrelsen såsom personuppgiftsbiträde för personuppgiftsbehandlingen.

Kommunstyrelsen har till Datainspektionen gett in avtal och utskrifter av avtalsvillkor mellan kommunen och dess personuppgiftsbiträden. Följande villkor, utdrag och avtal har getts in avseende Google Apps,

a) Google Apps general terms – security and compliance SLA,
b) Google Non-Disclosure Agreement,
c) Conditions for Personal Data Assistants (as a subsection),
d) Google Apps for business via reseller agreement ingånget med Google Inc och
e) Google Apps general terms, ingånget med Google Ireland Limited

I svar på Datainspektionens fråga har kommunstyrelsen uppgett att huvudavtalet är *Google Apps for business via reseller agreement* (avtal d). Vid inspektionstillfället angav kommunstyrelsen att det dokument, som ingivits och som benämns *Conditions for Personal Data Assistans,* utgör kommunens personuppgiftsbiträdesavtal med Google. I ett kompletterande yttrande från kommunstyrelsen anges att detta dokument ska ses som ett förtydligande av huvudavtalet om vad som utgör kommunens personuppgiftsbiträdesavtal. I dokumentet anges parterna YY och XX. Vidare hänvisas i dokumentet till olika avsnitt i *Google Apps for business via reseller agreement* (avtal d) och revisionsprogrammet SAS 70 typ II.

Google Apps general terms (avtal e) är ett tilläggsavtal mellan kommunstyrelsen och Google Ireland Ltd.

I avtalet mellan kommunen och Google Ireland Ltd har Datainspektionen uppmärksammat följande avtalsvillkor

1.4 Privacy Policies. Customer acknowledges that it has chosen to have its End Users personal data processed by Google as part of the Services within the scope of the Services' capabilities, which are reflected in the Google Privacy Policies. Customer therefore instructs Google to provide the Services and process End User personal data in accordance with the Google Privacy Policies and Google agrees to do the same. The Google Privacy Policies are hereby incorporated by reference into this Agreement. Customer agrees to protect the privacy of End Users by complying with a policy communicated to End Users which is no less protective than the Google Privacy Policies.1.5

1.5 Data Protection. In Section 1.4 and Section 1,5, the terms"personal data", "processing", "data controller" and "data processor" shall have the meanings ascribed to them in the EU Directive. For the purposes of this Agreement and in respect of the personal data of End Users, the parties agree that Customer shall be the data controller and Google shall be a data processor. Google shall take and implement appropriate technical and organisational measures to protect such personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

16.3 Sub-contracting. Either Party may sub-contract its obligations under this Agreement, in whole or in part, without the prior written consent of the other, provided that the sub-contracting party remains fully liable for all such sub-contracted obligations and accepts full liability as between the parties for the actions and/or inactions of its sub-contractors as if such actions and/or inactions were its own.

Kommunstyrelsen har uppgett att enligt avtal med Google ska Google behandla alla personuppgifter själva. Kommunstyrelsen har i telefonsamtal uppgett att all data hanteras av Google Inc och dess dotterbolag och att Google inte anlitar några underleverantörer utanför koncernen.

Ändring av avtal

Kommunstyrelsen uppgav vid inspektionen att Google förbehåller sig rätten att ändra avtalet. Kommunen måste dock informeras om någon avtalsförändring görs. Kommunen har, bl.a. med anledning av detta, tecknat avtalstider på ett år och en uppsägningstid på en månad. Detta framgår av ingivet avtal *Google Apps for business via reseller Agreement* avsnitt 1.2 *Modifications.*

I den Privacy policy som kommunstyrelsen länkat till framgår att denna kan komma att ändras.

Behandling av personuppgifter i Google Apps

Utöver de personuppgifter som kan komma att behandlas i samband med att e-post skickas och kalendern eller chatten används, kan personuppgifter om

användaren komma att behandlas av kommunstyrelsen, för administration och kontroll.

Kommunen har en policy för Internet och e-post. I denna finns bl.a. följande avsnitt.

> *Sekretess*
> All elektronisk sänd information kan läcka till andra än den tänkta mottagaren. Därför ska inte sekretessbelagd information sändas som e-post

IT-säkerhet

Datainspektionen har vid inspektionen och efterföljande skriftväxling ställt frågor om såväl organisatoriska som tekniska säkerhetsåtgärder.

Kommunen följer BITS-konceptet (Basnivå för informationssäkerhet) i sitt säkerhetsarbete. Kommunen har en IT-säkerhetsplan som uppdaterades under 2010 och ska följas upp under 2011. Hela regelverket finns tillgängligt på kommunens intranät. IT-avdelningen har informationsmöten med förvaltningscheferna. Det krävs formella beslut av ledningsgruppen eller styrelsen när en ny tjänst ska användas.

Kommunen genomförde en förenklad risk- och sårbarhetsanalys inför beslutet om införande av Google Apps. Kommunen började med ENISA-modellen, men ansåg sig inte behöva följa den fullt ut eftersom de inte tänker överföra något känsligt material.

Behörighetsstyrning

Kommunen har idag en katalogstruktur baserad på organisationstillhörighet. Genom rollhantering kommer metakatalogen att styra behörigheterna automatiskt. Informationen till metakatalogen hämtas från personalsystemet. De anställda vid kommunen som har behörighet att utföra administrativa uppgifter, är de som är anställda vid IT-verksamheten i kommunen. Verksamhetssystemen Lön och Skola hanteras inte i Google Apps eller Google Docs utan återfinns i egen miljö. Dessa program administreras enligt kommunens systemförvaltningsplan. Skoldatasystemet har för närvarande ingen koppling till metakatalogen.

Behörigheter kan slås av och på av kommunstyrelsen i den administrativa panelen hos Google. Administratörerna kan skapa grupper som i den administrativa panelen kan ges tillgång till olika applikationer. Vid tidpunkten för inspektionen hade i princip alla grupper tillgång till samma applikationer. Det

finns tre grupper för olika chefer där behörigheterna är kopplade till delegationsordningen.

Administratörer kan inte göra något med de personuppgifter de har tillgång till i Google Apps annat än kontrolladministration. Det är bara den anställde som kan se innehållet i sitt e-postkonto. Administratörer kan bara ta del av innehållet om de byter den anställdes lösenord och därefter loggar in.

Inloggning
För att komma in i Google Apps måste användarna först logga in i kommunens IT-system och därefter i Google Apps. Lösenorden autogenereras. Kraven på hur lösenordet måste vara sammansatt är desamma för inloggning i kommunens IT-system som i Google Apps. Det finns regler för lösenordens sammansättning. I Google finns en ”sparfunktion” men den har kommunen inaktiverat. Lösenordet lagras krypterat. För kommunens anställda gäller att det är tvingande lösenordsbyte var 30:e dag och att de senaste tio lösenorden inte kan återanvändas vid lösenordsbyte. Elever har samma lösenord under hela terminen eftersom de har tillgång till en annan typ av uppgifter och som inte omfattas av sekretesskyddat.

Det finns olika möjligheter att ge administratörerna en tvåfaktorslösning för inloggning. Vid inspektionen uppgav kommunstyrelsen att de planerade att ha en sådan på plats när systemet ska börja användas.

Google för en logg på misslyckade inloggningsförsök som kommunen kan begära ut från Google. Det kommer upp ett meddelande efter tredje misslyckade inloggningsförsöket, men det finns ingen spärr som förhindrar fortsatta inloggningsförsök.

Loggning
Google loggar inloggningar, vilken IP adress som använts samt vilka applikationer som körts.

Kommunikation och skydd av uppgifter
Kommunen krypterar inga uppgifter, men uppgifterna förs över till Google genom en krypterad förbindelse. Kommunstyrelsen har angivit att kommunikationen mellan Google Apps och kommunen skyddas genom SSL med dubbelsidig serverautentisering.

Back up
Enligt avtalet med Google ska uppgifterna finnas sparade på flera ställen samtidigt.

Fysisk säkerhet
Kommunstyrelsen har uppgett att den enligt SAS 70 har rätt till tillträde till Googles lokaler för att kontrollera hur kommunstyrelsens uppgifter lagras. Vidare har kommunstyrelsen hänvisat till Googles egen information om säkerheten för Google Apps på en av Googles webbsidor.

Utplåning
Google ska radera all information och överföra den till kommunen om kommunen väljer att avsluta avtalet. All information som en avslutad användare har genererat – i mejl och kalender – ligger kvar hos Google i 60 dagar innan kontot tas bort.

Överföring till tredje land
Uppgifterna lagras på flera ställen, men enligt avtalet ska uppgifterna lagras inom EU/EES-området eller inom USA där Safe Harbor-principerna gäller eftersom Google är ansluten till Safe Harbor.

Enligt amerikanska handelsdepartementets hemsida är Google Inc ansluten till Safe Harbor principerna.

Skäl för beslutet

Tillsynsbeslutets omfattning
Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen. Datainspektionen tar i det här beslutet inte ställning till om molntjänstanvändningen är förenlig med andra bestämmelser än dem i personuppgiftslagen. Det kan finnas bestämmelser i till exempel offentlighets- och sekretesslagen (2009:400), som begränsar möjligheten för kommunstyrelsen att lämna ut uppgifter för behandling av andra.

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.

Kommunen har anlitat Google för att tillhandahålla funktionerna e-post, kalender och chat för anställda och elever. Datainspektionens beslut omfattar endast kommunstyrelsens anställdas användning av dessa funktioner.

Kommunstyrelsen är den som bestämt att kommunstyrelsens anställda ska använda de av Google tillhandahållna tjänsterna.

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

Kommunstyrelsen har uppgett att personuppgifter kan komma att behandlas av andra bolag än Google Ireland Ltd – av Google Inc. och dess dotterbolag. Det har i ärendet framkommit att kommunstyrelsen inte har kunskap om vilka bolag inom Google koncernen som behandlar uppgifter för deras räkning.

Datainspektionen konstaterar att samtliga bolag inom Googlekoncernen som behandlar eller kan komma att behandla 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 registrerades personliga integritet (missbruksregeln). Personuppgiftslagens säkerhetsbestämmelser i 30 -32 §§ är dock, enligt 5 a § tillämpliga, oavsett vilket av de två regelsystemen som är tillämpligt. Avsikten med missbruksregeln är enligt förarbetena att undanta t.ex. en enskild medarbetares egen sedvanliga användning av datorstödd kommunikation, inte att undanta en organisations registrering av medarbetarnas kommunikation (prop. 2005/06:173 s. 23).

Kommunstyrelsens anställdas sedvanliga användning av e-postprogram kan således omfattas av missbruksregeln. Detta gäller under förutsättning att uppgifterna och meddelandena inte ingår eller avses ingå i mer kvalificerade system med personuppgiftsanknuten strukturering t.ex. dokument eller ärendehanteringssystem.

Den personuppgiftsbehandling som den personuppgiftsansvarige utför i samband med administration och kontroll av anställda såsom uppläggning av konton, autentisering och behörighetskontroll, har som regel en personuppgiftsanknuten struktur.

Datainspektionen konstaterar att hanteringsreglerna gäller för kommunstyrelsens behandling för administration och kontroll av e-post, kalender och chat.

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, tredjelandsöverföring 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 anlitandet 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 anlitanden 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.

Personuppgiftslagens krav på säkerhet vid behandling av personuppgifter

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 försämras 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 säkerhetsgärder 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.

Kravet på skriftligt personuppgiftsbiträdesavtal, 30 § personuppgiftslagen

Kommunstyrelsen har uppgett att personuppgifter kan komma att behandlas av Google Inc. och dess dotterbolag. I enlighet med vad som ovan konstaterats är alla bolag som behandlar personuppgifter för kommunstyrelsens räkning att betrakta som personuppgiftsbiträden till kommunstyrelsen.

Krav på personuppgiftsbiträdesavtal med underleverantörer

Datainspektionen har tidigare ansett att det krävs att den personuppgiftsansvarige själv ingår avtal med varje personuppgiftsbiträde/underbiträde för att uppfylla kravet i 30 § andra stycket personuppgiftslagen. Kravet på personuppgiftsbiträdesavtal kan enligt Datainspektionen dock uppfyllas även genom att den personuppgiftsansvarige ger ett personuppgiftsbiträde mandat att ingå avtal med underbiträden. Detta gäller under förutsättning att det föreskrivs att underbiträdena är skyldiga att följa den personuppgiftsansvariges instruktioner och att varje personuppgiftsbiträde också föreskrivs vara skyldiga att uppfylla de säkerhetskrav som den personuppgiftsansvarige ska uppfylla en-

ligt 31 § personuppgiftslagen. Dessutom måste kommunstyrelsen säkerställa att den har kännedom om vilka personuppgiftsbiträden som kan komma att behandla kommunstyrelsens personuppgifter.

Det har i ärendet framkommit att kommunstyrelsen inte har kunskap om vilka bolag inom Google-koncernen som behandlar personuppgifterna för deras räkning. De skrivningar som finns i ingivna avtal om informationsdelning och anlitande av underleverantörer är inte godtagbara.

Datainspektionen bedömer därför att kommunstyrelsen inte lever upp till personuppgiftslagens krav på personuppgiftsbiträdesavtal. Det gör ingen skillnad för bedömningen i detta fall att samtliga bolag som behandlar personuppgifterna ingår i samma koncern.

Datainspektionen konstaterar, på grund av det ovan sagda, att ingivna avtal mellan kommunstyrelsen och Google inte lever upp till kraven på personuppgiftsbiträdesavtal i 30 § andra stycket personuppgiftslagen.

Datainspektionen förelägger därför kommunstyrelsen att upprätta personuppgiftsbiträdesavtal som lever upp till kraven i personuppgiftslagen.

Personuppgiftsbiträdesavtal upprättas antingen genom tecknande av ett avtal med varje bolag inom Googlekoncernen som behandlar personuppgifter för kommunstyrelsens räkning, eller genom att i ett avtal ge Google Ireland Ltd eller Google Inc mandat att ingå ett avtal med underbiträden där det förskrivs att varje personuppgiftsbiträde har samma skyldigheter som det personuppgiftsbiträde som kommunstyrelsen ingår avtal med.

Kommunstyrelsen måste dessutom säkerställa att den har kännedom om vilka personuppgiftsbiträden som kan komma att behandla kommunstyrelsens personuppgifter.

Krav på personuppgiftsbiträdesavtal och dess innehåll
Det finns krav både på att det ska finnas personuppgiftsbiträdesavtal och på att den personuppgiftsansvarige ska ha kontroll över sina personuppgiftsbiträden. Självfallet måste det också ställas vissa krav på innehållet i avtalet.

En grundförutsättning är att avtalet och dess innehåll är urskiljbart från övriga villkor som gäller mellan parterna och att det kan visas upp för tillsynsmyndigheten. Kommunstyrelsen har uppgett att det ingivna dokumentet *Conditions for personal data assistans* utgör ett personuppgiftsbiträdesavtal. Data-

inspektionen kan inte se vem som skulle kunna anses bunden av detta avtal. De ingivna handlingar som tydligast reglerar personuppgiftsbehandling är avtalet med Google Ireland Ltd, *Google Apps Genaral Terms*, avsnitt 1.4 och 1.5, och den Privacy Policy som det där hänvisas till. Kommunstyrelsen har i ärendet gett in ett antal olika dokument som innehåller mängder av olika avtalsvillkor. Kommunstyrelsen har dock inte kunnat redogöra för vilka delar i dessa som utgör kommunstyrelsens personuppgiftsbiträdesavtal. Det har i ärendet varit fråga om en stor mängd olika avtal med olika hänvisningar. Ett sätt att göra avtalsvillkoren i personuppgiftsbiträdesavtalet urskiljbara från övriga avtalsvillkor är att kommunstyrelsen ser till att i en separat handling teckna ett personuppgiftsbiträdesavtal med sina personuppgiftsbiträden.

Datainspektionen konstaterar, på grund av det ovan sagda, att ingivna avtal mellan kommunstyrelsen och Google inte lever upp till kraven på personuppgiftsbiträdesavtal i 30 § andra stycket personuppgiftslagen.

Datainspektionen anser att villkoren i personuppgiftsbiträdesavtalet ska vara urskiljbara från övriga villkor som gäller mellan parterna.

Datainspektionen anser vidare att kravet i 30 § andra stycket personuppgiftslagen innebär att personuppgiftsbiträden inte ensidigt ska kunna förändra förutsättningarna för personuppgiftsbehandlingen så att skyddet för personuppgifter försämras.

Ingivna avtal till Datainspektionen kan, genom Googles i avtalen inkorporerade Privacy Policy, ändras ensidigt av Google. Privacy Policyn innehåller följande skrivning: ”Observera att Privacy policyn kan komma att ändras från tid till annan. Vi kommer inte att begränsa dina rättigheter enligt denna sekretesspolicy utan ditt uttryckliga samtycke.”

Datainspektionen konstaterar att det finns utrymme för Google Ltd. och Google Inc. att på eget initiativ och självständigt ändra villkoren och att det är otydligt hur stora förändringar Googlebolagen kan göra utan kommunstyrelsens samtycke.

Datainspektionen konstaterar, på grund av det ovan sagda, att ingivna avtal mellan kommunstyrelsen och Google inte lever upp till kraven på personuppgiftsbiträdesavtal i 30 § andra stycket personuppgiftslagen.

Datainspektionen anser att personuppgiftsbiträdesavtalets villkor inte ensidigt ska kunna förändras av personuppgiftsbiträdet.

Det är viktigt att inte bara reglera behandlingen av personuppgifter under ett avtals giltighet. Det är också viktigt att reglera vad som ska hända med personuppgifterna när avtalet upphör. När avtalet upphör saknar personuppgiftsbiträdet normalt grund för att fortsätta behandla personuppgifterna.

Datainspektionen anser att personuppgiftsbiträdesavtalet ska säkerställa att parterna vet vilka åtgärder som ska vidtas vid avtalets upphörande så att personuppgiftsbiträdet inte längre har åtkomst till personuppgifterna därefter.

Svensk lag
Kommunstyrelsen måste alltid följa svensk dataskyddslagstiftning. Det innebär en skyldighet för kommunstyrelsen att se till att de personuppgiftsbiträden som anlitas också gör det.

Datainspektionen anser att det i personuppgiftsbiträdesavtalet ska föreskrivas att personuppgiftsbiträdet är skyldigt att tillämpa svensk lagstiftning när det gäller behandlingen av personuppgifter.

Avtalet och lämpliga säkerhetsåtgärder enligt 31 § personuppgiftslagen
Vidare ska avtalet fastställa att personuppgiftsbiträdet är skyldigt att vidta lämpliga säkerhetsåtgärder enligt 31 § personuppgiftslagen.

I ingivna handlingar (*Google Apps Genaral Terms*) finns skrivningar där det framgår att Google ska tillhandahålla tjänsten och behandla personuppgifter i enlighet med Googles Privacy Policies, som genom en hänvisning även införlivas i avtalet. Det framgår vidare att Google ska vidta och genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter mot oavsiktlig eller olaglig förstörelse, förlust, ändring eller åtkomst. Kommunstyrelsen måste, mot bakgrund av att villkoren är skrivna av Google, granska de avtalsvillkor som Google anger och utifrån dessa bedöma, om de personuppgifter som kommunstyrelsen tänker behandla i Google Apps kommer att skyddas på ett tillfredsställande sätt.

Datainspektionen anser att personuppgiftsbiträdesavtalet ska föreskriva att personuppgiftsbiträdet är skyldigt att vidta lämpliga säkerhetsåtgärder enligt 31 § personuppgiftslagen.

Datainspektionen anser att personuppgiftsbiträdesavtalet ska säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstanke om obehörig åtkomst av personuppgifter inom kommunen eller hos Googleföretagen.

För Datainspektionens granskning av vidtagna säkerhetsåtgärder, se avsnittet ”IT-säkerhet” nedan.

Behandling endast för berättigade ändamål
I 9 § personuppgiftslagen ställs grundläggande krav som måste uppfyllas vid all personuppgiftsbehandling. Bl.a. får personuppgifter bara behandlas om det är lagligt, de får bara samlas in för särskilda, uttryckligen angivna och berättigade ändamål och får inte behandlas för något ändamål som är oförenligt med det för vilket personuppgifterna samlades in. Ett personuppgiftsbiträdesavtal ska säkerställa att personuppgiftsbiträdet endast behandlar personuppgifter i enlighet med personuppgiftsansvariges instruktioner och därmed fastställa att personuppgiftsbiträdet inte får behandla personuppgifter för egna eller andra ändamål än dem som den personuppgiftsansvarige anlitat personuppgiftsbiträdet för.

Någon sådan skrivning finns inte i de av kommunstyrelsen ingivna handlingarna. Den avtalskonstruktion som Google använder sig av vid tillhandahållande av Google Apps innefattar inte heller, såvitt Datainspektionen förstår, några möjligheter för kunden, i det här fallet kommunstyrelsen, att ge några egna instruktioner eller att själv ange vilka säkerhetsåtgärder som den anser vara lämpliga för att skyddet av personuppgifter inte ska försämras då Google behandlar personuppgifterna. Kommunstyrelsen kan endast granska de avtalsvillkor som Google anger och utifrån dessa bedöma för vilka ändamål Google kommer att behandla kommunstyrelsens personuppgifter. Av Googles Privacy Policy framgår att denna gäller för ”alla produkter, tjänster och webbplatser från Google Inc. eller dess dotterbolag eller närstående företag med undantag för Postini”. Policyn innehåller skrivningar om hur Google avser att samla in, använda och dela information. Vidare finns skrivningar om att inhämtad information kan användas för att ”förbättra våra tjänster (inklusive annonstjänster) och utveckla nya tjänster".

Det saknas tydliga skrivningar som säkerställer att personuppgiftsbiträdet inte får behandla personuppgifterna för andra ändamål än de som kommunstyrelsens bestämt.

Datainspektionen konstaterar, på grund av det ovan sagda, att ingivna avtal mellan kommunstyrelsen och Google inte lever upp till kraven på personuppgiftsbiträdesavtal i 30 § andra stycket personuppgiftslagen.

Datainspektionen anser att det i personuppgiftsbiträdesavtalet ska föreskrivas att Googleföretagen endast får behandla personuppgifter i enlighet med kommunstyrelsens instruktioner och därmed säkerställa att personuppgifts-

biträdet inte behandlar personuppgifter för andra ändamål än dem som kommunstyrelsen anlitat biträdet för.

Kravet på kontroll av personuppgiftsbiträden
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 data lagras eller bearbetas rent fysiskt och därmed även geografiskt. Om en molnleverantör utan användarens vetskap kan flytta data inte bara mellan olika underleverantörer utan 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.

Kommunstyrelsen har i ärendet framfört att den med stöd av ett SAS 70 –avtal har rätt till tillträde till Googles lokaler för att kontrollera hur data lagras. Datainspektionen kan av den ingivna dokumentationen inte utläsa att så är fallet och ifrågasätter om ett sådant förfarande som kommunstyrelsen hänvisar till skulle vara lämpligt, eftersom data från flera aktörer lagras i samma lokaler och tillträdesmöjligheter för alla som lagrar data skulle innebära säkerhetsrisker i sig.

Att använda sig av tredjepartsrevision kan vara ett sätt att kontrollera att leverantören och tjänsten uppfyller vissa säkerhets- och kvalitetskrav. Det fråntar dock inte den personuppgiftsansvarige från sitt ansvar att kontrollera att personuppgiftsbiträden både kan och verkligen vidtar säkerhetsåtgärder i enlighet med 31 § personuppgiftslagen. Kommunstyrelsen är skyldig att säkerställa att den på lämpligt sätt har möjlighet att följa upp att dess personuppgiftsbiträden lever upp till villkoren i avtalet.

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

Datainspektionen konstaterar att kommunstyrelsen inte lever upp till kraven i 31 § andra stycket personuppgiftslagen eftersom kommunstyrelsen inte har kunskap om vilka bolag inom personuppgiftsbiträdets koncern som behandlar personuppgifterna för dennes räkning lever.

Datainspektionen anser att kommunstyrelsen måste säkerställa att den på lämpligt sätt har möjlighet att följa upp att personuppgiftsbiträden lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen vidtar lämpliga säkerhetsåtgärder.

Förbudet mot överföring till tredje land

Hanteringsreglerna gäller för kommunstyrelsens behandling för administration och kontroll av e-post, kalender och chat. Enligt 33 § personuppgiftslagen är det förbjudet att till tredje land föra över personuppgifter som är under behandling om landet inte har en adekvat nivå för skyddet av personuppgifterna. Vissa undantag från överföringsförbudet finns i personuppgiftslagen och personuppgiftsförordningen (1998:1191). Undantag gäller bl.a. om EG-kommissionen konstaterat att det tredje landet har en adekvat skyddsnivå eller om den organisation som personuppgifterna förs över till har anslutit sig till de s.k. Safe Harbor-principerna i USA.

Kommunstyrelsen har uppgett att personuppgifterna lagras på flera ställen, men enligt avtal ska personuppgifterna lagras inom EU/EES-området eller inom USA. En överföring av personuppgifter till datacenter belägna i USA omfattas av förbudet i 33 § personuppgiftslagen. Kommunstyrelsen har uppgett att Google Inc. har anslutit sig till Safe Harbor-principerna, vilket även framgår på Federal Trade Commissions hemsida. Det är därför tillåtet att föra över personuppgifter från EU/EES till Google Inc. i USA. Såvitt framgår i ärendet kan kommunstyrelsens personuppgifter behandlas även av andra bolag i USA än av Google Inc. Datainspektionen anser inte att det är klarlagt att dessa andra bolag är anslutna till Safe Harbor-principerna.

Datainspektionen förlägger kommunstyrelsen att förvissa sig om att alla bolag som behandlar kommunstyrelsens personuppgifter i tredje land har anslutit sig till Safe Harbor-principerna eller att överföringen är tillåten på någon annan grund.

IT-säkerhet

Det är alltid kommunstyrelsen som ytterst har ansvaret för att personuppgifterna skyddas när personuppgiftsbiträden anlitas.

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.

Kommunikationssäkerhet
Personuppgifter som överförs via Internet eller andra öppna nät bör, beroende på känsligheten hos personuppgifterna, skyddas mot avlyssning, förvanskning och ändring. Detta kan ske till exempel genom kryptering. Ju känsligare personuppgifter som behandlas desto högre krav ställs på säkerhetsåtgärder. Det finns ett antal grundläggande säkerhetsbrister i de kommunikationsprotokoll som ligger till grund för e-postsystem.

När ett e-postmeddelande överförs mellan avsändare och mottagare kan det passera, och lagras på, ett antal servrar längs vägen. Ett mottaget e-postmeddelande ligger kvar på e-postserverarna och kan ofta nås på flera sätt, t.ex. över Internet. En kopia av det skickade e-postmeddelandet ligger vanligen kvar även hos avsändaren. Om informationen i e-postmeddelandet är okrypterad eller på annat sätt oskyddad, finns det risk att obehöriga kan ta del av informationen vid var och en av dessa servrar. Det finns heller inga möjligheter att utan extra åtgärder säkerställa att adressaten är den tänkta mottagaren.

Datainspektionen har, i ett tidigare beslut rörande en socialnämnds användning av e-post, angett att personuppgifter som är känsliga enligt 13 § personuppgiftslagen endast får lämnas ut via öppna nät till identifierade användare vars identitet är säkerställd med en teknisk funktion som kryptering, engångslösenord eller motsvarande. Känsliga personuppgifter ska dessutom vid överföring via öppet nät, till exempel Internet, förses med krypteringsskydd. Datainspektionen har också ansett att även andra personuppgifter som annars är särskilt känsliga, som t.ex. uppgifter om lagöverträdelser och uppgifter som är sekretessreglerade, ska krypteras när de skickas med e-post.

Enligt 30 1 st § personuppgiftslagen får den eller de personer som arbetar under biträdets eller den personuppgiftsansvariges ledning bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Kommunstyrelsen krypterar inga uppgifter i e-post, men vid administration och inloggning förs uppgifter över till Google via Internet genom en krypterad förbindelse. Kommunstyrelsen har en e-postpolicy i vilken det anges att sekretesskyddade uppgifter inte ska skickas med e-post.

Datainspektionen erinrar kommunstyrelsen om att den måste se över sin e-postpolicy och tydligt instruera sina medarbetare om vilka personuppgifter som inte får skickas med e-post utan att de först krypteras.

Inloggning och lösenord

Känsliga personuppgifter, enligt 13 § personuppgiftslagen, får endast lämnas ut via öppna nät till identifierade användare vars identitet är säkerställd genom stark autentisering som t.ex. e-legitimation, engångslösenord eller motsvarande. Även åtkomst till andra integritetskänsliga personuppgifter kan kräva starka autentiseringslösningar. Vid inspektionen framkom att användare och administratörer loggar in till tjänsterna via Internet, och att båda dessa användargrupper autentiserar sig med användarnamn och lösenord. Datainspektionen har inget att anmärka på inloggningslösningen avseende tjänsterna e-post, chat och kalender under förutsättning att inga känsliga personuppgifter behandlas.

Vid kommunens planerade användning av andra tjänster än e-post, kalender och chat måste kommunen se till att inloggning sker genom stark autentisering om den kommande behandlingen innebär behandling av känsliga personuppgifter.

Behörighetsstyrning

Vid inspektionen framkom att det är ett begränsat antal administratörer hos kommunen som har behörighet till den administrativa panelen i Google Apps. Administratörerna kan skapa grupper som i den administrativa panelen kan ges tillgång till olika applikationer. Datainspektionen har inget att anmärka när det gäller behörighetstilldelning avseende e-post, chat och kalender.

Med hänsyn till kommunens planerade användning vill Datainspektionen i detta sammanhang påminna om följande. I 9 § personuppgiftslagen finns grundläggande krav på behandlingen av personuppgifter. En princip som följer av de grundläggande kraven i 9 § är att anställda och andra inte ska ta del av, eller på annat sätt, behandla fler personuppgifter än vad som är nödvändigt för att de ska kunna utföra sitt arbete. De grundläggande kraven i 9 § personuppgiftslagen gäller i princip för behandlingen av alla slags personuppgifter, det vill säga även för personuppgifter som inte omfattas av sekretess. Register och dokument- och ärendehanteringssystem hos en kommun, innehåller ofta stora mängder personrelaterad information. Personuppgiftslagens krav på lämpliga säkerhetsåtgärder, i 31 §, medför att myndigheten ska ha ett system för behörighetsstyrning för att begränsa den elektroniska tillgången till personuppgifter i sådana system och register. Med hjälp av detta bör åt-

komstmöjligheterna tekniskt begränsas så mycket som det är faktiskt och praktiskt möjligt med hänsyn till den aktuella verksamheten och känsligheten hos personuppgifterna. Därutöver ska kommunen förhindra obehörig åtkomst genom fungerande rutiner, t.ex. arbetsrutiner, rutiner för utbildning och information till anställda samt rutiner för åtkomstkontroll. Behovet av åtkomst varierar naturligtvis beroende på vilket verksamhetsområde det är fråga om och den anställdes arbetsuppgifter.

Loggar och logguppföljning
Kommunstyrelsen har uppgett att Google loggar vilken användare som nyttjat en viss applikation och menar att det följer av SAS 70 typ II att kommunstyrelsen när som helst kan begära ut loggar från Google. Initialt planerar kommunstyrelsen bara att genomföra loggkontroller på förekommen anledning. När alla systemen är överförda till Google Apps ska rutinmässiga kontroller göras.

Datainspektionen har inte kunnat skapa sig någon närmare kännedom om hur de loggar som kommunstyrelsen angett att Google för är utformade. Inte heller har Datainspektionen kunnat verifiera att kommunstyrelsen på begäran kan få ut loggar från Google.

Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring, förlust, ändringar, otillåten spridning eller otillåten tillgång till uppgifterna. Det ställs högre krav på dessa åtgärder om behandlingen innefattar överföring av personuppgifter via öppna nät. Kommunstyrelsen måste därför säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstanke om obehörig åtkomst av personuppgifter inom Kommunstyrelsen eller hos Google.

Loggkontroll av e-postsystem ska kunna ske på förekommen anledning. Därav följer att kommunstyrelsen ansvarar för att se till att det finns loggar och att loggarna kan användas för att utreda obehörig åtkomst – oavsett om personen som haft åtkomst till personuppgifterna befinner sig hos kommunen eller hos Google.

Kommunstyrelsen måste därför säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstanke om obehörig åtkomst av personuppgifter inom kommunen eller hos Googleföretagen.

Utplåning
Ett grundläggande krav i personuppgiftslagen är att personuppgifter inte ska bevaras under en längre tid än vad som är nödvändigt med hänsyn till ända-

målet med behandlingen. Den personuppgiftsansvarige ska således tillse att, när personuppgifter inte längre används för sitt ändamål, lagringsmedierna antingen förstörs eller raderas på sådant sätt att personuppgifterna inte kan återskapas. Kommunstyrelsen har angett att den genom sitt avtal med Google reglerat att uppgifter ska raderas. Det är viktigt att reglera detta och att personuppgifterna raderas hos alla eventuella personuppgiftsbiträden.

Risk- och sårbarhetsanalys

I ärendet har framkommit att kommunen avser att använda fler tjänster under 2011 – Google Presentation och Google Docs, kalkyl och text. Datainspektionen har också uppfattat att kommunen som helhet avser att helt gå över till molnbaserade tjänster och att IT-verktyg som socialtjänst, vård och skola använder sig av ska läggas ut sist, senast 2015. Om den planerade användningen innebär att personuppgifter i stor mängd och av känsligare karaktär behandlas, medför det stora integritetsrisker, vilket höjer säkerhetskraven. För att kommunstyrelsen ska kunna ta ställning till vilka säkerhetsåtgärder som måste vidtas, behöver kommunen genomföra en ordentlig risk- och sårbarhetsanalys av den behandlingen.

Datainspektionen har i sina allmänna råd uttalat att det finns flera etablerade metoder för risk- och sårbarhetsanalyser. När man använder dessa metoder, särskilt de som baseras på checklistor, är det viktigt att komma ihåg att det ofta är fråga om generella riktlinjer. Styrkan med metoderna är att någon redan har tänkt igenom olika situationer som kan uppstå. Man får stöd så att inte något viktigt glöms bort. Dessutom går man systematiskt till väga när man arbetar efter en redan fastlagd metod. Nackdelen med att använda en checklista är att det finns en 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*.)

Datainspektionen erinrar kommunstyrelsen om att den måste genomföra en risk- och sårbarhetsanalys gällande personuppgiftsbehandling för kommunstyrelsens framtida användning av molntjänster.

Den planerade användningen

Beträffande annan användning av molntjänster än kommunstyrelsens användning av Google Apps tjänster för kalender, e-post och chat vill Datainspektionen sammanfattningsvis uppmärksamma kommunstyrelsen och övriga personuppgiftsansvariga nämnder inom Salems kommun på följande.

Risk och sårbarhetsanalys

Datainspektionen uppfattar att Salem kommuns planerade användning utöver användningen av tjänsterna e-post, kalender och chat kan komma att innebära behandling av personuppgifter i stor mängd och av känslig karaktär. Sådan behandling medför stora integritetsrisker. All sådan användning måste föregås av att kommunen gör en ordentlig risk- och sårbarhetsanalys.

Instruktioner

För att minska integritetsriskerna är den personuppgiftsansvariges instruktioner till användarna viktiga. För kommande användning är det viktigt att kommunen ger tydliga instruktioner till sina anställda om vilka personuppgiftsbehandlingar som är tillåtna och under vilka förutsättningar anställda får ta del av personuppgifter.

Ytterligare säkerhetsåtgärder

Utöver de brister som framförts ovan i beslutet bör kommunen, beroende på personuppgifternas mängd och känslighet, överväga om ytterligare säkerhetsåtgärder är nödvändiga. Vid behandling av känsliga personuppgifter gäller:

- Högre krav på autentisering
- Högre krav på behörighetsstyrning
- Högre krav på loggar och logguppföljning för att utreda, och i vissa fall förebygga, obehörig åtkomst

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 överklagandet 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-säkerhetsspecialisterna Adolf Slama och Magnus Bergström, samt juristerna Lena Carlsson och Ulrika Andersson, föredragande.

Göran Gräslund Ulrika Andersson

Kopia till: Personuppgiftsombudet