Datainspektionen

Datum	Diarienr
2013-05-31	1351-2012

Kommunstyrelsen i
Salems kommun
144 80 Rönninge

Tillsyn enligt personuppgiftslagen (1998:204) – Uppföljning av beslut i ärende 263-2011

Datainspektionens beslut

Datainspektionen konstaterar att personuppgiftsbiträdesavtalet som Kommunstyrelsen i Salems kommun avser att teckna med molntjänst-leverantören

1. inte uppfyller kraven på instruktioner till biträdet vad avser ändamål med behandling och radering av personuppgifter, och
2. inte garanterar kommunstyrelsen tillräcklig insyn i vilka under-leverantörer som anlitas.

Datainspektionen förelägger kommunstyrelsen att upphöra med behandlingen av personuppgifter i molntjänsten, eller att

1. vidta åtgärder för att instruktionerna i personuppgiftsbiträdesavtalet ska vara förenliga med personuppgiftslagen, och
2. säkerställa att kommunstyrelsen har kännedom om vilka under-leverantörer som anlitas.

Ärendet avslutas.

Redogörelse för tillsynsärendet

Bakgrund

Datainspektionen har i ett tidigare ärende (dnr 263-2011) granskat kommun-styrelsens i Salems kommun (kommunstyrelsen) användning av molntjänsten Google Apps.

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

I beslut den 28 september 2011 förelades kommunstyrelsen att upprätta ett personuppgiftsbiträdesavtal som lever upp till kraven i personuppgiftslagen (PuL).

Avtalet ska bland annat

- föreskriva att biträdet endast får behandla personuppgifter i enlighet med kommunstyrelsens instruktioner och därmed säkerställa att biträdet inte behandlar personuppgifter för andra ändamål än dem som kommunstyrelsen anlitat biträdet för,
- säkerställa att parterna vet vilka åtgärder som ska vidtas vid avtalets upphörande så att biträdet inte längre har åtkomst till personuppgifterna därefter,
- säkerställa att kommunstyrelsen har kännedom om vilka personuppgiftsbiträden som kan komma att behandla kommunens personuppgifter.

Kommunstyrelsen förelades också att förvissa sig om att alla bolag i tredje land som behandlar personuppgifter åt kommunstyrelsen antingen är anslutna till Safe Harbor-principerna eller att överföringen är tillåten på annan grund.

Under detta ärendes handläggning har kommunstyrelsen yttrat sig och inkommit med handlingar som ligger till grund för beslutet. Även molntjänsteleverantören och övriga europeiska dataskyddsmyndigheter har givits tillfälle att yttra sig i ärendet.

De avtal kommunstyrelsen gett in till Datainspektionen är ännu inte ingångna mellan parterna.

Datainspektionens beslut omfattar enbart kommunstyrelsens användning av e-post och kalender som molntjänst.

Kommunstyrelsens avtalsparter och aktuella avtal
Följande avtal och bilagor har beaktats i beslutet.

1. Google Apps Enterprise via Reseller Agreement (huvudavtal)
2. Data Processing Addendum (bilaga till huvudavtalet, s.k. personuppgiftsbiträdesavtal)
3. Appendix: Security Measures
4. EU- kommissionens standardavtalsklausuler (2010/87/EU) för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG

5. Google Privacy Policy

Enligt kommunstyrelsens uppgift gäller i första hand huvudavtalet och dess bilaga jämte standardavtalsklausulerna. För det fall det finns motstridiga villkor i Privacy Policyn i förhållande till övriga nämnda avtal gäller vad som stadgas i de sistnämnda.

Kommunstyrelsen har för avsikt att teckna avtal (huvudavtal och bilaga) med Google Ireland Limited och att ingå EU-kommissionens standardavtals-klausuler med Google Inc. i USA.

Skäl för beslutet och bedömning

Risk- och sårbarhetsanalys
Datainspektionen konstaterar att kommunstyrelsen genomfört en risk- och sårbarhetsanalys. Datainspektionen rekommenderar att kommunstyrelsen fortlöpande arbetar med riskidentifiering och säkerhetsutvärdering i sin risk- och sårbarhetsanalys.

Av 31 § PuL framgår att den personuppgiftsansvarige ska vidta lämpliga organisatoriska säkerhetsåtgärder. Att genomföra en risk- och sårbarhets-analys är ett exempel på en sådan säkerhetsåtgärd.

För att en personuppgiftsansvarig ska kunna bedöma om det är möjligt att anlita en molntjänstleverantör måste först en grundlig risk- och sårbarhets-analys genomföras. Syftet med en sådan analys är bland annat att synliggöra och skapa medvetenhet om de risker som finns med den tänkta person-uppgiftsbehandlingen. Analysen bör resultera i en förteckning över vilka sårbarheter och risker som finns och vilka säkerhetsåtgärder som kan vidtas för att förhindra att dessa risker realiseras.

Den personuppgiftsansvarige måste också skapa utrymme i sin organisation för att fortlöpande arbeta med säkerhetsfrågor. Risk- och sårbarhetsanalysen ska vara ett stöd i detta arbete och ska uppdateras kontinuerligt i samband med exempelvis organisatoriska förändringar hos den ansvarige, ändringar i användningen av molntjänsten eller annat som påverkar riskbilden för de uppgifter som hanteras.

Det finns en mängd olika metoder för att utföra en risk- och sårbarhetsanalys. Grundläggande är dock att utgå ifrån den egna verksamhetens behov och förutsättningar och den behandling av personuppgifter som är planerad. Dessa förhållanden ska sedan ställas i relation till de avtalsvillkor och säker-hetsåtgärder molntjänstleverantören erbjuder och de säkerhetsåtgärder den

ansvarige själv kan vidta. Själva analysen görs därefter i ljuset av personuppgiftslagen och/eller annan tillämplig lagstiftning.

En risk- och sårbarhetsanalys kan omfatta följande moment.

Riskidentifiering

- Vilka personuppgifter kommer att behandlas i molntjänsten?
- Vem eller vilka hos den personuppgiftsansvarige kommer att behandla personuppgifterna?
- Vilka risker finns med personuppgiftsbehandlingen?

Riskanalys

- Hur sannolikt är det att respektive risk kommer att realiseras?
- Vad blir konsekvenserna för de registrerade om en risk realiseras?
- Vad blir konsekvenserna för den personuppgiftsansvarige om en risk realiseras?

Utvärdering

- Vilka åtgärder kan den personuppgiftsansvarige vidta för att förhindra att risker realiseras?
- Vilket skydd för personuppgifter erbjuder molntjänstleverantören i sina avtalsvillkor?
- Överensstämmer skyddet för personuppgifter som den personuppgiftsansvarige och molntjänstleverantören vidtar med de krav som ställs i personuppgiftslagen och/eller annan tillämplig lagstiftning?

Personuppgiftsbiträdesavtalet

Ett personuppgiftsbiträde och den eller de personer som arbetar under biträdet får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. I ett personuppgiftsbiträdesavtal ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet är skyldigt att vidta de säkerhetsåtgärder som följer av bestämmelserna i PuL.

Instruktionerna till biträdet ska vara så pass tydliga att otillåten behandling av uppgifterna inte kommer att utföras. Det förhållandet att den ansvarige hanterar personuppgifter i s.k. ostrukturerat material (5 a § PuL) fråntar inte den ansvarige skyldigheten att se till att biträdet har klara instruktioner för sin behandling av personuppgifter. Sådana instruktioner ska exempelvis omfatta ändamål med behandling av personuppgifter och hur länge uppgifterna får bevaras hos biträdet.

Kommunstyrelsens behandling av personuppgifter i e-post- och kalenderfunktioner omfattar såväl strukturerat som ostrukturerat material i PuL:s mening. I det följande är Datainspektionens utgångspunkt att kommunstyrelsens instruktioner till personuppgiftsbiträdet ska omfatta all personuppgiftsbehandling som förekommer i tjänsterna, dvs. såväl i strukturerad som i ostrukturerad form.

1. Instruktioner till biträdet - Ändamål med behandling av personuppgifter

Datainspektionen konstaterar att kommunstyrelsens instruktioner till personuppgiftsbiträdet om ändamålen för behandling av personuppgifter är för vida och ger utrymme för biträdet att behandla personuppgifter för egna ändamål.

1.1 Lagtext m.m.

Ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal (personuppgiftsbiträdesavtal) om biträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet ska det särskilt föreskrivas att biträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet är skyldigt att vidta de säkerhetsåtgärder som anges i 31 § första stycket PuL (30 § PuL).

Instruktionerna till biträdet om ändamålen med behandlingen ska utgå ifrån den personuppgiftsansvariges ändamål med sin tänkta hantering av personuppgifter. Instruktionerna får inte omfatta befogenhet för biträdet att exempelvis behandla personuppgifterna på ett sätt som inte skulle vara tillåtet för den ansvarige.

29-gruppen pekar i sitt yttrande om datormoln[1] (avsnitt 3.4.1.2) på att det inte är ovanligt att ett typiskt molnscenario omfattar ett stort antal underentreprenörer. Risken för att personuppgifter kan komma att behandlas för andra, oförenliga ändamål måste därför, enligt yttrandet, betraktas som ganska stor.

1.2 Parternas avtal och yttranden

Av 6.1 i bilagan till huvudavtalet framgår att molntjänstleverantören;

”will process Customer Personal Data for the purposes of providing, maintaining and improving the services”

[1] Artikel 29-arbetsgruppen för skydd av personuppgifter, yttrande 5/2012 om datormoln (cloud computing).

Av Privacy Policyn framgår mer i detalj hur molntjänstleverantören hanterar sina kunders personuppgifter.

Kommunstyrelsen har i ett yttrande den 1 mars 2013 inkommit med ett förslag till omskrivning av instruktioner om ändamålen för behandlingen.

I ett yttrande den 6 maj 2013 har kommunstyrelsen anfört att ändamålsbeskrivningen i biträdesavtalet är adekvat och tillräckligt tydlig. Vidare uppges att molntjänstleverantören antytt att normalt sett används bara kommunstyrelsens personuppgifter för utveckling av kommunstyrelsens individuella tjänster. Kommunstyrelsen och molntjänstleverantören har efter diskussion kommit fram till att personuppgifterna är tillräckligt skyddade och endast används för ett syfte som är väsentligt för IT-utvecklingen i samhället.

1.3 Datainspektionens bedömning

Syftet med integritetsskyddslagstiftningen är att skydda den enskilde från onödiga, eller onödigt stora, intrång i den personliga integriteten. Grundläggande i lagstiftningen är att en enskild ska ha rätt att få information om *hur* hans eller hennes personuppgifter behandlas och i förekommande fall kunna välja att avstå från att få sina uppgifter behandlade. För att en enskild ska ha förutsättningar att göra ett välgrundat ställningstagande krävs dock att den personuppgiftsansvarige kan informera om för vilka specifika ändamål personuppgifter behandlas. En ändamålsbeskrivning kan därför inte vara alltför diffust formulerat utan måste ha en viss grad av precision.

Utgångspunkten i ett förhållande mellan en personuppgiftsansvarig och ett personuppgiftsbiträde är att biträdet inte har rätt att behandla den ansvariges uppgifter för egna ändamål. En generell observation från inspektionens sida är emellertid att förhållandet mellan en ansvarig och en molntjänstleverantör ofta regleras av ett standardavtal. I ett sådant avtal anges i regel inte den ansvariges ändamål med personuppgiftsbehandlingen. Instruktionerna till biträdet i standardavtal är istället formulerade på ett sätt som möjliggör för biträdet att behandla den ansvariges personuppgifter för egna ändamål. Sådana ändamål kan exempelvis vara att utveckla eller förbättra leverantörens molntjänster. Även mellan kommunstyrelsen och den i detta ärende aktuella molntjänstleverantören är det leverantören som specificerat instruktionerna i avtalet.

Att behandla personuppgifter för att utveckla och förbättra tjänster kan i och för sig vara förenligt med PuL om ändamålet och personuppgifterna som hanteras är tydligt avgränsat. För att uppnå detta krävs klara instruktioner om exempelvis

- vilka, eller vilka kategorier, av personuppgifter som behandlas för ändamålet,
- från vilka av den personuppgiftsansvariges behandlingar som personuppgifter används, och
- för utveckling/förbättring av vilken typ av tjänster eller kategorier av tjänster som leverantören använder den ansvariges uppgifter.

Om den ansvarige instruerar biträdet att behandla personuppgifter för att utveckla och förbättra tjänster är det den personuppgiftsansvarige som ansvarar för att skydda den enskildes integritet vid denna behandling. Enligt Datainspektionens bedömning är såväl de befintliga instruktionerna som de nya som föreslagits om ändamål för behandling alltför vida och lämnar utrymme för biträdet att behandla personuppgifterna i egna syften. Instruktionerna uppfyller därmed inte kraven i PuL.

2. Instruktioner till biträdet - Lagring av personuppgifter

Datainspektionen konstaterar att kommunstyrelsens instruktioner till personuppgiftsbiträdet om radering av personuppgifter lämnar utrymme för biträdet att fortsätta behandla uppgifter som raderats av den ansvarige.

2.1 Lagtext m.m.

Ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal (personuppgiftsbiträdesavtal) om biträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet ska det särskilt föreskrivas att biträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet är skyldigt att vidta de säkerhetsåtgärder som anges i 31 § första stycket PuL (30 § PuL).

Instruktionerna till biträdet om radering av personuppgifter måste utgå ifrån att när den ansvarige har markerat personuppgifter för radering ska biträdet inom en rimlig tidsperiod, påbörja slutlig radering av informationen i fråga. Utgångspunkten är att när personuppgifter har markerats för radering får de inte längre behandlas på annat sätt än som ett led i raderingsprocessen.

Radering av uppgifter innebär antingen att uppgifterna raderas helt från det medium där de lagras eller att de avidentifieras på ett sådant sätt att de inte är möjliga att koppla till en enskild individ eller går att återskapa.

Av 29-gruppens yttrande[2] (avsnitt 3.4.1.3) framgår att det är den personuppgiftsansvarige som bör se till att molntjänstleverantören garanterar säker radering och att avtalet mellan leverantören och kunden innehåller tydliga bestämmelser om radering av personuppgifter.

2.2 Parternas avtal och yttranden

Av 9.1 i bilagan till huvudavtalet framgår att molntjänstleverantören under avtalstiden;

"will provide Customer with the ability to export and delete Customer Data in a manner consistent with the functionality of the Services"

I samma paragraf framgår att molntjänstleverantören efter att avtalet upphört eller avslutats;

"will delete Customer Data in accordance with the terms of the Agreement".

I standardavtalet regleras under punkten 11 effekter av uppsägning av avtalet (11.3). Däri anges att personuppgifter kommer att raderas

"after a commercially reasonable period of time"

Under samma avsnitt redogörs för att personuppgifterna kommer att raderas genom att de över tid skrivs över med andra data.

Av Privacy Policyn framgår att

"after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup system"

Kommunstyrelsen har i yttrande den 6 maj 2013 anfört att de principer för gallring som molntjänstleverantören har tydliggjort är tillräckliga för att uppnå ett gott integritetsskydd i personuppgiftsbehandlingarna som utförs.

Molntjänstleverantören har i ett yttrande den 20 april 2013 föreslagit en uppdaterad skrivning i avtalet angående radering av uppgifter. Enligt den föreslagna formuleringen får personuppgifter som markerats för radering av den ansvarige endast behandlas för vissa givna ändamål exempelvis när åtgärder behöver vidtas i säkerhetssyfte och vissa andra specificerade ändamål.

---

[2] Artikel 29-arbetsgruppen för skydd av personuppgifter, yttrande 5/2012 om datormoln (cloud computing).

2.3 Datainspektionens bedömning

En enskild ska kunna känna sig trygg med att uppgifter som raderats av den personuppgiftsansvarige inte fortsätter att bevaras eller behandlas hos personuppgiftsbiträdet. När den ansvarige begär radering av uppgifter i en molntjänst signalerar det till biträdet att uppgifterna snarast ska utplånas eller avidentifieras. Givetvis är det acceptabelt att biträdets radering av personuppgifter sker med en viss fördröjning. Biträdet ska dock kunna förvissa den ansvarige om att uppgifterna raderas inom en viss angiven tid.

Det saknas uppgift om hur länge molntjänstleverantören bevarar uppgifter som har raderats av kommunstyrelsen. Det är också oklart hur länge leverantören kommer att bevara kommunstyrelsens personuppgifter efter att avtalet mellan parterna har upphört.

Enligt Datainspektionens bedömning är kommunstyrelsens instruktioner till biträdet om när personuppgifter ska raderas inte förenliga med PuL. Detta gäller såväl de nu gällande villkoren som de nya som föreslagits av molntjänstleverantören. Datainspektionens uppfattning är att leverantörens föreslagna ändring är ett steg i rätt riktning. Det saknas dock fortfarande garantier för radering av uppgifterna. Den nya versionen innehåller också formuleringar som, beroende på hur de tolkas, öppnar upp för leverantören att fortsätta behandla uppgifter som markerats för radering. Kommunstyrelsens instruktioner till biträdet måste omfatta uppgift om genomsnittlig eller maximal lagringstid. Även en förhållandevis lång maximal lagringstid bör vara godtagbar så länge biträdet ges instruktioner om att uppgifter som har markerats för radering av den ansvarige enbart får behandlas för ändamål som är motiverade av säkerhetsskäl eller som ett led i raderingen av uppgifterna i fråga.

3. Underleverantörer

Datainspektionen konstaterar att, såvitt inspektionen erfar, parternas avtal inte ger förutsättningar för kommunstyrelsen att uppfylla kraven på kontroll av biträden i 31 § andra stycket PuL.

3.1 Lagtext m.m.

Av 31 § andra stycket PuL framgår att den personuppgiftsansvarige ska förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att biträdet verkligen vidtar åtgärderna.

I 29-gruppens yttrande[3] (avsnitt 3.3.2) framgår att om ett personuppgiftsbiträde använder sig av underleverantörer är biträdet skyldigt att ge kunden tillgång till information om detta och beskriva

- vilken typ av tjänst som underleverantören utför,
- vilka egenskaper nuvarande eller potentiella underleverantörer har, samt
- vilka garantier som uppställs för att dataskyddsdirektivet (94/46/EG) kommer att följas.

Av yttrandet framgår också att ett personuppgiftsbiträde bara får lägga ut sin verksamhet på underentreprenörer om den personuppgiftsansvarige har lämnat sitt samtycke till detta. Den personuppgiftsansvarige kan lämna ett generellt samtycke när tjänsten börjar tillhandahållas.

Personuppgiftsbiträdet har en tydlig skyldighet att informera den ansvarige om eventuella planerade ändringar t.ex. att underentreprenörer läggs till eller tas bort. Den personuppgiftsansvarige ska hela tiden ha möjlighet att invända mot ändringarna eller säga upp avtalet. Det bör finnas en tydlig skyldighet för molnleverantören att ange alla underentreprenörer som anlitas.

3.2 Parternas avtal och yttranden

I avsnitt 12 i bilagan till huvudavtalet anges att leverantören kan använda sig av andra bolag eller underleverantörer i koncernen för att tillhandahålla tjänsten till kunden. I 12.3 i bilagan stadgas att kunden samtycker till att leverantören använder sig av underleverantörer. Av artikel 15.3 i huvudavtalet framgår att;

”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”.

Via en länk kan den ansvarige få åtkomst till en webbsida varifrån molntjänstleverantören tillhandahåller en lista över vilka bolag som kan anlitas som underleverantörer för kundsupport. Molntjänstleverantören eller någon av dess dotterbolag kan även anlita underleverantörer för att utföra andra tjänster. Vilka bolag som kan komma ifråga här anges dock inte. Som underleverantörer listas inte heller bolag inom den egna koncernen. Däremot finns

[3] Artikel 29-arbetsgruppen för skydd av personuppgifter, yttrande 5/2012 om datormoln (cloud computing).

information, på en annan webbsida som tillhandahålls av leverantören, om var leverantörens serverhallar är belägna runt om i världen. Molntjänstleverantören lämnar inga garantier för uppgifternas riktighet.

Kommunstyrelsen har i yttrande den 6 maj 2013 anfört att de anser sig ha tillräcklig information om molntjänstleverantörens underleverantörer för att kunna utöva ansvar och kontrollera informationssäkerhetsåtgärder. Vid osäkerhet var personuppgifterna lagras kan kommunstyrelsen alltid, enligt avtal, få ett förtydligande från molntjänstleverantören.

3.3 Datainspektionens bedömning

Användningen av molntjänster involverar en rad olika aktörer och var och en av dessa har olika roller. Ansvaret för behandlingen av personuppgifter gentemot den registrerade åvilar dock som regel bara den personuppgiftsansvarige. Detta oavsett var och av vem den faktiska behandlingen utförs. Det är den ansvarige som ska se till att föreliggande avtal och partsförhållanden säkerställer att samtliga personuppgiftsbiträden följer integritetsskyddslagstiftningen. Det är också den ansvarige som ska se till att de registrerade kan utöva sina rättigheter såsom rätt till information och rättelse (26 och 28 §§ PuL). För att den personuppgiftsansvarige ska kunna garantera att registrerade kan tillvarata sina rättigheter måste den ansvarige ha kännedom om *vilka underleverantörer* som behandlar den registrerades personuppgifter och *var dessa underleverantörer är lokaliserade.*

Den lista på underleverantörer som tillhandahålls av molntjänstleverantören är otillräcklig i det avseendet att det inte anges var respektive företag är lokaliserat. Listan utgör inte heller en tillräcklig garanti för att den ansvarige vid alla tider ska ha kännedom om var personuppgifterna behandlas. Bedömningen görs mot bakgrund av att leverantören inte garanterar att listan är fullständig, korrekt och uppdaterad. Under sådana förhållanden kan den personuppgiftsansvarige inte uppfylla kraven i 31 § andra stycket PuL. Datainspektionen kan inte heller se att de bifogade avtalen innehåller villkor om kommunstyrelsens rätt att kräva förtydligande information från molntjänstleverantören. Ett avtalsvillkor om rätt till förtydligande information skulle dock kunna vara tillräckligt för att uppfylla kraven i PuL.

4. Överföring av personuppgifter till tredje land

Datainspektionen konstaterar att överföringen av personuppgifter till USA är tillåten med stöd av Safe Harbor-principerna.

Datainspektionen konstaterar att standardavtalsklausulerna utgör en laglig grund för överföring av personuppgifter till annat tredje land än USA under

förutsättning att den tillagda klausul 6.4 inte är i strid med någon bestämmelse i standardavtalsklausulerna.

4.1 Lagtext m.m.

Bestämmelserna om tredjelandsöverföring är endast tillämpliga på personuppgifter som hanteras i strukturerat material.

I personuppgiftslagen regleras överföring av personuppgifter till tredje land i 33 – 35 §§. Huvudregeln är att tredjelandsöverföring är förbjuden till länder som inte har en adekvat nivå för skyddet av personuppgifter. Överföring kan dock vara tillåtet till exempelvis bolag i USA som är anslutna till Safe Harbor-principerna eller om parterna använder sig av EU-kommissionens standardavtalsklausuler (2010/87/EU).

Vid användning av standardavtalsklausulerna får parterna inte ändra i klausulerna. Detta hindrar inte parterna från att, om nödvändigt, lägga till klausuler om affärsrelaterade frågor, så länge dessa inte står i strid med någon annan klausul (se klausul 10, i EU-kommissionens standardavtalsklausuler).

4.2 Parternas avtal och yttranden

I punkten 11 i bilagan till huvudavtalet regleras villkoren för överföring av personuppgifter till tredje land. Molnleverantörens bolag i USA är anslutet till Safe Harbor-principerna. För överföringen till bolag i andra länder utanför EU/EES-området har kommunstyrelsen valt att använda sig av EU-kommissionens standardavtalsklausuler (2010/87/EU). Standardavtalsklausuler kommer att tecknas med molnleverantörens bolag i USA som också ges mandat att teckna avtal med underleverantörer (12.3 i bilagan).

Molntjänstleverantören har gjort ett tillägg i standardavtalsklausulerna genom att föra in en ny klausul 6.4. I denna klausul begränsar leverantören sitt ansvar gentemot kommunstyrelsen enligt vad som framgår av bilagan till huvudavtalet. Såvitt Datainspektionen kan se saknas dock bestämmelser om ansvarsbegränsningar i bilagan. Under avsnitt 13 i huvudavtalet finns emellertid villkor om begränsning av parternas ansvar. I 13.4 anges följande.

"each party's liability under this Agreement (whether in contract, tort or otherwise) in relation to liability arising from any given event or series of connected events, shall be limited…"

Kommunstyrelsen har i yttrande anfört att klausul 6.4 redogör för Salems och molntjänstleverantörens amerikanska bolags ansvar gentemot varandra under huvudavtalet. I huvudavtalet regleras annars bara ansvaret mellan Salem och molntjänstleverantörens bolag på Irland.

4.3 Datainspektionens bedömning

För att standardavtalsklausulerna (2010/87/EU) ska utgöra en laglig grund för tredjelandsöverföring får inga ändringar eller tillägg som står i strid med klausulerna göras. Datainspektionen finner det oklart om tillägget är i strid med standardavtalsklausulerna eller inte. Men under förutsättning att klausul 6.4 inte står i strid med någon bestämmelse i standardavtals-klausulerna utgör dessa en laglig grund för överföring av personuppgifter till tredje land.

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 t.f. generaldirektören Hans-Olof Lindblom i närvaro av tillsynschefen Erik Janzon, IT-säkerhetsspecialisten Adolf Slama och juristen Ingela Alverfors (föredragande).

Hans-Olof Lindblom

Ingela Alverfors

Kopia till:

Personuppgiftsombudet