Datainspektionen

Datum	Diarienr
2014-04-25	1475-2013

Utbildningsnämnden
Ale kommun
449 80 Alafors

Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av personuppgifter i molntjänsten Office 365

Datainspektionens beslut
Datainspektionen konstaterar att personuppgiftsbiträdesavtalet som Utbildningsnämnden i Ale kommun har tecknat med sitt personuppgifts-biträde inte ger nämnden rätt till nödvändig information om i vilka länder biträdets underleverantörer är lokaliserade och behandlar personuppgifter.

Datainspektionen förutsätter att utbildningsnämnden vidtar nödvändiga åtgärder för att säkerställa att nämnden får tillgång till information om i vilka länder anlitade underleverantörer är lokaliserade och behandlar personuppgifter.

Ärendet kommer att följas upp.

1. Redogörelse för tillsynsärendet

Datainspektionen har granskat Utbildningsnämnden i Ale kommuns (härefter nämnden) behandling av personuppgifter i Microsofts molntjänst Office 365. Granskningen har utförts genom att nämnden skriftligen har fått svara på frågor och skicka in relevanta handlingar till Datainspektionen.

1.1 Ärendets avgränsning och definitioner

Syftet med Datainspektionens granskning har i första hand varit att kontrollera om nämndens personuppgiftsbiträdesavtal med molntjänst-leverantören Microsoft uppfyller personuppgiftslagens krav i förhållande till den behandling av personuppgifter nämnden planerar att utföra i molntjänsten.

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

Datainspektionen har inte granskat om nämndens behandling av personuppgifter i övrigt är förenlig med personuppgiftslagen.

En utgångspunkt för beslutet i detta ärende är att nämnden i molntjänsten endast behandlar personuppgifter som varken är känsliga i den mening som avses i 13 § personuppgiftslagen eller annars av integritetskänslig natur exempelvis uppgifter som omfattas av sekretess eller uppgifter som rör lagöverträdelser. Vidare har Datainspektionen förutsatt att nämnden behandlar personuppgifterna i såväl strukturerat som i ostrukturerat material (5 a § personuppgiftslagen).

Nämnden är personuppgiftsansvarig för behandlingen av personuppgifter i molntjänsten och benämns i beslutet som nämnden, den personuppgifts-ansvarige eller den ansvarige.

Molntjänstleverantören Microsoft är nämndens personuppgiftsbiträde och benämns i beslutet som molntjänstleverantören, personuppgiftsbiträdet eller biträdet.

Personuppgiftsbiträden som är underleverantörer till molntjänstleverantören benämns i beslutet som underleverantörer eller underentreprenörer.

1.2 Nämndens behandling av personuppgifter i Office 365

Nämnden har i huvudsak anfört följande.
Nämnden avser att använda Office 365 som ett pedagogiskt arbetsverktyg i all skol-, förskole- och fritidsverksamhet.

Nämndens ändamål med behandling av personuppgifter i molntjänsten är att

- stödja lärares pedagogiska arbete,
- lagra pedagogiskt material, och
- möjliggöra kommunikation mellan användarna.

Nämnden kommer inte att hantera elevadministration, individuella utvecklingsplaner eller personliga omdömen i molntjänsten.

Elever och medarbetare kommer att få tillgång till följande tjänster.

- SharePoint Online för samarbete, dokument- och informationsdelning.
- Skydrive Pro för organisering och lagring av dokument, bilder, filmer och annat pedagogiskt arbetsmaterial.
- Lync Online för snabbmeddelanden och videosamtal.

- Office Web Apps för tillgång till Word, PowerPoint, Excel och OneNote.

Eleverna kommer även tilldelas e-postkonton med kalenderfunktion via tjänsten Exchange Online.

Personuppgifter såsom namn, klass och skola behandlas i molntjänsten för att möjliggöra tillgång till arbetsverktygen. Andra personuppgifter kan förekomma i fritext. För att förhindra att känsliga personuppgifter behandlas i molntjänsten har nämnden tagit fram skriftliga instruktioner till användarna. Av instruktionerna framgår bland annat att känsliga personuppgifter inte får skrivas eller sparas i molntjänsten.

Nämnden har genomfört en risk- och sårbarhetsanalys och tecknat personuppgiftsbiträdesavtal med molntjänstleverantören.

1.3 Avtal och avtalsparter

Nämnden har uppgett att följande avtal har tecknats med personuppgiftsbiträdet.

- Microsoft Campus och School Avtal (generella villkor)
- Enrollment for Education Solutions (licensbeställning)
- Enrollment for Education Solutions Addendum Office 365 Data processing Agreement (with EU Standard Contractual Clauses) Amendment ID EES18 (personuppgiftsbiträdesavtal)
- Amendment to the Enrollment for Educational Solutions addendum, Office 365 Agreement, Amendment IC CTM (tillägg till personuppgiftsbiträdesavtalet)
- EU-kommissionens standardavtalsklausuler för överföring av personuppgifter till tredje land (2010/87/EU)
- Service Level Agreement for Microsoft Online Services

Samtliga avtal har ingåtts mellan nämnden och Microsoft Irland Operations Limited förutom EU-kommissionens standardavtalsklausuler för överföring av personuppgifter till personuppgiftsbiträden som är etablerade i tredje land (2010/87/EU) som har tecknats med Microsoft Corporation i USA.

Av personuppgiftsbiträdesavtalets avsnitt 7.c. framgår att vid händelse av motstridiga bestämmelser i ovan uppräknade avtal har villkoren i biträdesavtalet företräde.

I avtalen, och i nämndens yttranden, finns hänvisningar till bland annat följande relevanta dokument och webbplatser.

- Microsoft Online Information Security Policy
- Sekretesspolicy för Office 365
- Product Use Rights
- Microsoft Trust Center (webbplats)
- TechNet (webbplats)

2. Skäl för beslutet och bedömning

Artikel 29-gruppen[1] har tagit fram ett yttrande om molntjänster[2]. Yttrandet analyserar alla relevanta frågor som rör molntjänstleverantörer som bedriver verksamhet inom EES-området och deras kunder och innehåller rekommendationer och riktlinjer som är vägledande för samtliga medlemsländer inom EU. Artikel 29-gruppens rekommendationer och riktlinjer har varit vägledande för Datainspektionen i detta beslut.

2.1 Risk- och sårbarhetsanalys

Den personuppgiftsansvarige måste genomföra en risk- och sårbarhetsanalys för att bedöma om det är möjligt att anlita en molntjänstleverantör för en planerad behandling av personuppgifter.

2.1.1 Lagtext m.m.

Av 31 § personuppgiftslagen framgår att den personuppgiftsansvarige ska vidta lämpliga organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas.

Att genomföra en risk- och sårbarhetsanalys är ett exempel på en sådan organisatorisk säkerhetsåtgärd.

2.1.2 Datainspektionens bedömning

Datainspektionen ser positivt på att nämnden har genomfört en risk- och sårbarhetsanalys. Datainspektionen rekommenderar att nämnden fortlöpande arbetar med riskidentifiering och säkerhetsutvärdering i sin risk- och sårbarhetsanalys.

Behandling av personuppgifter i molntjänster som tillhandahålls över internet av globala molntjänstleverantörer kan medföra vissa specifika risker som den personuppgiftsansvarige måste beakta innan en planerad behandling av personuppgifter inleds. Riskerna hänför sig framför allt till bristande kontroll

[1] Artikel 29-arbetsgruppen är inrättad enligt artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet.
[2] Yttrande 5/2012 om datormoln (cloud computing), 01037/12/SV, WP 196, antaget den 1 juli 2012

över de personuppgifter som behandlas i molntjänsten och bristande insyn i personuppgiftsbiträdets behandling av personuppgifterna ifråga.

För att en personuppgiftsansvarig ska kunna bedöma om det är möjligt att behandla personuppgifter i en molntjänst måste den ansvarige först genomföra en grundlig risk- och sårbarhetsanalys. Analysen ska genomföras bland annat med beaktande av vilka personuppgifter som ska behandlas och vilken säkerhet molntjänstleverantören erbjuder. Därefter måste den ansvarige kontrollera om det, i förhållande till personuppgiftslagen och/eller annan tillämplig integritetsskyddslagstiftning, är tillåtet att behandla personuppgifter i molntjänsten, en s.k. laglighetsprövning. Risk- och sårbarhetsanalysen och laglighetsprövningen är ofta tätt sammanlänkade och kan med fördel genomföras inom ramen för samma utredning. För att den ansvarige ska kunna göra en välgrundad bedömning är det viktigt att molntjänstleverantören tillhandahåller alla nödvändiga avtalsdokument och all annan information som den ansvarige måste känna till om leverantörens behandling av personuppgifter och skyddet för dessa personuppgifter.

Enligt Datainspektionens uppfattning har nämnden genomfört en grundlig risk- och sårbarhetsanalys där bland annat sannolikheten för att en risk ska inträffa har bedömts i förhållande till vilken konsekvens det inträffade skulle medföra.

2.2 Allmänt om personuppgiftsbiträdesavtalet

Enligt 30 § personuppgiftslagen får ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets eller den personuppgiftsansvariges ledning behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige.

Det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 31 § första stycket.

Syftet med ett personuppgiftsbiträdesavtal är bland annat att ge garantier för att säkerhet och sekretess för personuppgifter inte ska påverkas negativt till följd av att den personuppgiftsansvarige väljer att anlita ett personuppgiftsbiträde istället för att själv utföra personuppgiftsbehandlingen. Enskilda vars personuppgifter behandlas ska alltså inte riskera att få ett sämre integritetsskydd för att den ansvarige väljer att låta personuppgifterna behandlas av ett biträde.

Tillsammans med övriga avtalsvillkor, policys och andra bindande dokument bidrar personuppgiftsbiträdesavtalet också till att öka transparensen i avtalsförhållandet och ge den ansvarige insyn i biträdets behandling av personuppgifter.

Den ansvariges instruktioner till biträdet i biträdesavtalet ska vara tillräckligt tydliga för att förhindra att biträdet exempelvis behandlar uppgifterna för egna ändamål. Det förhållandet att den ansvarige hanterar personuppgifter i ett ostrukturerat material fråntar inte den ansvarige skyldigheten att se till att biträdet har tydliga instruktioner för sin behandling av personuppgifterna. Biträdesavtalet ska också reglera vilka säkerhetsåtgärder biträdet ska vidta för att skydda de personuppgifter som behandlas.

Mot bakgrund av att många molntjänstleverantörer erbjuder sina kunder standardiserade avtalsvillkor är det av avgörande betydelse att den personuppgiftsansvarige utför en laglighetsprövning av avtalsvillkoren i förhållande till den planerade personuppgiftsbehandlingen. Endast på detta sätt kan den ansvarige kontrollera om den planerade behandlingen av personuppgifter i molntjänsten är tillåten enligt lag.

2.3 Instruktioner till biträdet – Ändamål med behandling av personuppgifter

Personuppgiftsbiträdet får bara behandla personuppgifterna enligt den personuppgiftsansvariges instruktioner. Instruktionerna till biträdet om för vilka ändamål personuppgifter får behandlas ska utgå ifrån den ansvariges ändamål med den tänkta hanteringen av personuppgifterna. Instruktionerna får inte omfatta befogenhet för biträdet att exempelvis behandla uppgifterna på ett sätt som inte skulle vara tillåtet för den ansvarige.

2.3.1 Lagtext m.m.

Bestämmelser om den personuppgiftsansvariges instruktioner till biträdet finns i 30 § personuppgiftslagen (se ovan under punkten 2.2).

2.3.2 Avtal och yttranden

Av nämndens yttrande framgår att ändamålen med behandlingen av personuppgifter i Office 365 är att tillhandahålla ett pedagogiskt arbetsverktyg som ska främja digitalt samarbete och kommunikation mellan lärare och elever.

Av avsnitt 2.b.(i) i personuppgiftsbiträdesavtalet framgår följande.

Customer Data will be used only to provide Customer the Office 365 Services. This may include troubleshooting aimed at preventing, detecting and repairing

problems affecting the operation of the Office 365 Services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam).

I tillägget till personuppgiftsbiträdesavtalet finns följande komplement till avsnitt 2.b.(i) i biträdesavtalet.

The Office 365 Services shall not capture, maintain, scan, index, share or use Customer Data, or otherwise use any data-mining technology, for any activity not authorized under the Agreement. Office 365 Services shall not use Customer Data for any advertising or other commercial purpose of Microsoft or any third party. Office 365 will be logically separate from Microsoft's consumer online services.

2.3.3 Datainspektionens bedömning

Datainspektionen bedömer att nämndens instruktioner i personuppgifts-biträdesavtalet och dess tillägg om hur biträdet får behandla personuppgifterna inte ger utrymme för biträdet att behandla uppgifterna för egna ändamål.

2.4 Instruktioner till biträdet - Lagring av personuppgifter

När den personuppgiftsansvarige har markerat personuppgifter för radering eller när avtalsförhållandet med personuppgiftsbiträdet upphör ska biträdet, inom en rimlig tidsperiod, påbörja slutlig radering av uppgifterna i fråga. Utgångspunkten måste i regel vara att när personuppgifter har markerats för radering får de inte längre behandlas av biträdet 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.

2.4.1 Lagtext m.m.

Bestämmelser om den personuppgiftsansvariges instruktioner till biträdet finns i 30 § personuppgiftslagen (se ovan under punkten 2.2).

Av artikel 29-gruppens yttrande (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.

2.4.2 Avtal och yttranden

Av avsnitt 2.c. i personuppgiftsbiträdesavtalet framgår följande.

Upon expiration or termination of Customer's use of the Office 365 Services, Customer may extract Customer Data and Microsoft will delete Customer Data.

Av tillägget till personuppgiftsbiträdesavtalet framgår följande.

Once Customer Data has been marked for deletion, Microsoft will process the Customer Data only for purposes of executing the deletion process, unless further processing is necessary to maintain the security or integrity of the Office 365 Services. Customer Data will be deleted within 180 days of having been marked for deletion.

2.4.3 Datainspektionens bedömning

Datainspektionen bedömer att nämndens instruktioner om radering av personuppgifter i personuppgiftsbiträdesavtalet och dess tillägg ger tillräckliga garantier för att personuppgiftsbiträdet raderar personuppgifterna inom en rimlig tidsperiod såväl under avtalstiden som efter avtalets upphörande.

2.5 Tekniska och organisatoriska säkerhetsåtgärder

Personuppgiftsbiträdet och dess underleverantörer är skyldiga att vidta lämpliga säkerhetsåtgärder för att skydda de personuppgifter som behandlas.

2.5.1 Lagtext m.m.

Bestämmelser om den personuppgiftsansvariges instruktioner till biträdet finns i 30 § personuppgiftslagen (se ovan under punkten 2.2).

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

a) de tekniska möjligheter som finns,
b) vad det skulle kosta att genomföra åtgärderna,
c) de särskilda risker som finns med behandlingen av personuppgifterna, och
d) hur pass känsliga de behandlade personuppgifter är.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, ska den personuppgiftsansvarige förvissa sig om att personuppgiftsbiträdet kan

genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Av artikel 29-gruppens yttrande (s. 14-16 och 20-22) framgår att de tekniska och organisatoriska säkerhetsåtgärderna ska säkerställa bland annat följande.

- Att den personuppgiftsansvarige har snabb och tillförlitlig tillgång till personuppgifterna.
- Att personuppgifterna är autentiska och inte med uppsåt eller oavsiktligt har ändrats under behandling, lagring eller överföring.
- Att personuppgifterna skyddas genom exempelvis kryptering.
- Att det finns nödvändig behörighetsstyrning hos såväl den personuppgiftsansvarige som hos personuppgiftsbiträdet.
- Att den behandling som utförs av personuppgiftsbiträdet och dess underleverantörer loggas.
- Att den personuppgiftsansvarige har rätt att själv eller genom tredje part granska personuppgiftsbiträdets behandling av personuppgifter.

För att även underleverantörer ska vara skyldiga att vidta samma säkerhets-åtgärder bör biträdet teckna ett avtal med varje underentreprenör som återspeglar villkoren i biträdets avtal med den personuppgiftsansvarige

2.5.2 Avtal och yttranden

I avsnitt 5 i personuppgiftsbiträdesavtalet redogörs för vilka säkerhetsåtgärder personuppgiftsbiträdet vidtar för att skydda personuppgifterna som behandlas. Där framgår bland annat att

- anställda hos biträdet lyder under sekretesskrav (5.a.(i)2),
- personuppgifter krypteras (5.a.(ii) 2) A.) och 5.a.(v) 4) A. och B.),
- det finns rutiner för behörighetsstyrning och behörighetstilldelning (5.a.(vi) 2 – 3)
- loggar förs (5.a. (v) 2)E. och 5.a. (vii) 1) B.), och att
- tredjepartsrevision genomförs i vart fall årligen enligt ISO 27001 standard. Den personuppgiftsansvarige kan skriftligen begära att få ta del av en sammanfattning av revisionsrapporten (5.b.(ii) och (iii)).

På begäran av den personuppgiftsansvarige tillhandahåller personuppgifts-biträdet en säkerhetspolicy som på ett mer detaljerat sätt beskriver de säkerhetsåtgärder biträdet vidtar för att skydda personuppgifter. I policyn finns bland annat information om biträdets rutiner för loggning, behörighetstilldelning och hantering av säkerhetsincidenter.

2.5.3 Datainspektionens bedömning

Datainspektionen bedömer att nämndens instruktioner om vilka säkerhetsåtgärder personuppgiftsbiträdet ska vidta är tillräckliga för att skydda de personuppgifter som nämnden avser att behandla i tjänsten.

Vilken säkerhet som krävs för att skydda personuppgifter beror på olika faktorer. Att personuppgifterna är känsliga eller sekretessreglerade är sådana faktorer liksom mängden uppgifter och antalet personer som uppgifterna avser. Enligt Datainspektionens bedömning är de säkerhetsåtgärder som vidtas tillräckliga mot bakgrund av att nämnden enbart behandlar uppgifter som varken är känsliga eller integritetskänsliga.

2.6 Överföring av personuppgifter till tredje land

När personuppgifter behandlas av personuppgiftsbiträden i ett land utanför EU/EES måste den personuppgiftsansvarige se till att något av undantagen från förbudet mot överföring till tredje land kan tillämpas.

2.6.1 Lagtext m.m.

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. Förbudet gäller också överföring av personuppgifter för behandling i tredjeland.

Enligt 13 § personuppgiftsförordningen (1998:1191) får personuppgifter föras över till tredjeland

1. om och i den utsträckning Europeiska kommissionen har konstaterat att landet har en adekvat nivå för skyddet av personuppgifter i enlighet med artikel 25.6 i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter eller
2. om personuppgifterna förs över med tillämpning av ett avtal som innehåller sådana standardavtalsklausuler som kommissionen enligt 26.4 i direktivet har beslutat erbjuder tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter.

2.6.2 Avtal och yttranden

Av personuppgiftsbiträdesavtalet, avsnitt 2.e[3] framgår följande.

[3] Avsnittsmarkeringen är felaktigt angiven som 2.a. i det bifogade personuppgiftsbiträdesavtalet men har uppdaterats i senare versioner av avtalet.

Customer Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Affiliates or subcontractors maintain facilities. Customer appoints Microsoft to perform any such transfer of Customer Data to any such country and to store and process Customer Data in order to provide the Office 365 Services.

Av samma avsnitt i biträdesavtalet framgår att Microsoft är anslutet till Safe Harbor-principerna och att överföring av personuppgifter till andra tredje länder än USA regleras genom att parterna tecknar EU-kommissionens standardavtalsklausuler.

Nämnden har i yttrande den 25 november 2013 anfört att inga ändringar eller tillägg har gjorts i standardavtalsklausulerna.

Nämnden har i yttrande den 27 februari 2014 anfört att biträdets underleverantörer i tredje länder är bundna av såväl standardavtalsklausulerna som åtagandena i personuppgiftsbiträdesavtalet (inklusive Safe Harbor-principerna). Detta framgår av de åtaganden i standardavtalsklausulerna som gäller vid sidan av personuppgiftsbiträdesavtalet (EES18).

2.6.3 Datainspektionens bedömning

Datainspektionen konstaterar att nämndens överföring av personuppgifter till Microsoft i USA är tillåten med stöd av Europeiska kommissionens beslut 2000/520/EG av den 26 juli 2000 avseende Safe Harbor-principerna.

Datainspektionen konstaterar att nämndens överföring av personuppgifter till andra tredje länder än USA är tillåten med stöd av Europeiska kommissionens beslut 2010/87/EU av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland.

2.7 Underleverantörer

Molntjänstleverantören och alla dess underleverantörer är personuppgiftsbiträden till den personuppgiftsansvarige. Den ansvarige måste förvissa sig om att det finns möjlighet att följa upp att samtliga biträden verkligen vidtar de säkerhetsåtgärder som krävs.

2.7.1 Lagtext m.m.

Av 31 § andra stycket personuppgiftslagen 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.

Av artikel 29-gruppens yttrande (avsnitt 3.3.2) framgår 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.

Vidare framgår (avsnitt 4.1) att utlämning av uppgifter till tredje part bör regleras endast genom avtalet. Avtalet bör omfatta en skyldighet för leverantören att ange alla sina underentreprenörer och se till att kunden får information om alla ändringar så att kunden kan göra invändningar mot ändringarna eller säga upp avtalet.

Biträdet är skyldigt att ge kunden tillgång till information om underleverantörer 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 (avsnitt 3.3.2).

Av yttrandet framgår vidare (avsnitt 4.1) att kunderna särskilt bör informeras om alla underentreprenörer som bidrar till att tillhandahålla den berörda molntjänsten och alla lokaler [översatt från engelskans ”locations”] där uppgifter kan komma att lagras eller behandlas av molnleverantören och/eller dennes underentreprenörer (särskilt om någon eller några lokaler ligger utanför Europeiska ekonomiska samarbetsområdet (EES)).

2.7.2 Avtal och yttranden

Enligt avsnitt 2.e.[4] i personuppgiftsbiträdesavtalet uppdrar den personuppgiftsansvarige åt personuppgiftsbiträdet att anlita underleverantörer för att behandla personuppgifter.

Av avsnitt 2.g.[5] i personuppgiftsbiträdesavtalet framgår följande.

Microsoft may hire other companies to provide limited services on its behalf, such as providing customer support.

[4] Avsnittsmarkeringen är felaktigt angiven som 2.a. i det bifogade personuppgiftsbiträdesavtalet men har uppdaterats i senare versioner av avtalet

[5] Avsnittsmarkeringen är felaktigt angiven som 2.f. i det bifogade personuppgiftsbiträdesavtalet men har uppdaterats i senare versioner av avtalet.

Av avsnitt 4.e. i personuppgiftsbiträdesavtalet framgår följande.

At least 14 days before authorizing any new subcontractor to access Customer Data, Microsoft will update the applicable website and provide notice to all customers that have subscribed to compliance notifications, as described in the website. If a Customer does not approve of a new subcontractor, then customer may terminate the affected Microsoft Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval.

På webbplatsen Microsoft Trust Center finns ett dokument vari samtliga aktuella underleverantörer är angivna. Underleverantörerna namnges och grupperas efter vilken typ av uppdrag de utför åt molntjänstleverantören. På samma webbplats finns också information om i vilka städer de datacenter är lokaliserade i vilka de personuppgifter nämnden behandlar lagras i första hand.

2.7.3 Datainspektionens bedömning

Datainspektionen konstaterar att personuppgiftsbiträdesavtalet som nämnden har tecknat med sitt personuppgiftsbiträde inte ger nämnden rätt till nödvändig information om i vilka länder personuppgiftsbiträdets underleverantörer är lokaliserade och behandlar personuppgifter.

Datainspektionen förutsätter att nämnden vidtar nödvändiga åtgärder för att säkerställa att nämnden får tillgång till information om i vilka länder anlitade underleverantörer är lokaliserade och behandlar personuppgifter.

Användningen av molntjänster involverar en rad olika aktörer och var och en av dessa har olika roller. Underleverantörer kan vara dotterbolag till molntjänstleverantören eller från molntjänstleverantören helt fristående bolag. Oavsett vilken ställning underleverantören har måste personuppgifts-biträdet tillhandahålla information om vilka bolag som är underleverantörer, var de är lokaliserade och deras huvudsakliga uppgift. Sådan information är avgörande för transparensen i avtalsförhållandet.

Personuppgiftsbiträdet tillhandahåller två olika informationskanaler för att informera om vilka underleverantörer som anlitas. När det gäller biträdets egna datacenter får nämnden information om var dessa är lokaliserade. Övriga underleverantörer anges enbart med firmanamn och typ av uppdrag som utförs. Information om var bolagen är lokaliserade saknas. Avsaknaden av denna uppgift reducerar nämndens insyn i biträdets personuppgifts-behandling och nämndens möjligheter att i enlighet med 31 §

personuppgiftslagen kontrollera dess personuppgiftsbiträden. För att nämnden ska kunna utöva kontroll och avgöra om det exempelvis finns anledning att motsätta sig att en viss underleverantör anlitas måste nämnden, enligt Datainspektionens uppfattning, i vart fall få kännedom om i vilket land respektive underleverantör är lokaliserad och behandlar personuppgifter. Denna information är nödvändig för att den ansvarige exempelvis ska kunna vidta åtgärder om det finns skäl att misstänka att uppgifter som behandlas i ett visst land inte åtnjuter ett tillräckligt skydd trots vad som anges i avtalen.

Hur man överklagar
Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska 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 Kristina Svahn Starrsjö efter föredragning av juristen Ingela Alverfors. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, t.f. enhetschefen Anna Hörnlund och IT-säkerhetsspecialisten Fredrik Ekman deltagit.

Kristina Svahn Starrsjö

Ingela Alverfors