Datainspektionen

Datum	Diarienr
2014-06-10	358-2014

Grundskolenämnden i Malmö Stad
Stadshuset
August Palms plats 1
205 80 Malmö

Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av personuppgifter i molntjänsten Google Apps For Education

Datainspektionens beslut

Datainspektionen konstaterar att personuppgiftsbiträdesavtalet som Grundskolenämnden i Malmö Stad tecknat med molntjänstleverantören inte uppfyller kraven på instruktioner till personuppgiftsbiträdet vad avser ändamålen med behandlingen av personuppgifter.

Datainspektionen förelägger nämnden att upphöra med behandlingen av personuppgifter i molntjänsten eller ta fram tydligt avgränsade instruktioner i personuppgiftsbiträdesavtalet avseende för vilka ändamål personuppgifts-biträdet får behandla personuppgifter. Instruktionerna ska vara i linje med nämndens egna ändamål för behandling och förenliga med personuppgiftslagen.

Om nämnden tar fram nya instruktioner i personuppgiftsbiträdesavtalet förutsätter Datainspektionen att nämnden också vidtar åtgärder för att tilldela superadmin och skoladmin individuella inloggningsuppgifter till respektive adminkonto.

Datainspektionen förutsätter också att nämnden kan få omedelbar tillgång till information om personuppgiftsbiträdets samtliga underleverantörer, var de är lokaliserade och vilken typ av uppdrag de utför.

Ärendet avslutas.

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

1. Redogörelse för tillsynsärendet

Datainspektionen har granskat Grundskolenämnden i Malmö Stads (härefter nämnden) behandling av personuppgifter i molntjänsten Google Apps For Education. Granskningen har genomförts genom en inspektion på plats hos nämnden. Nämnden har yttrat sig över protokollet från inspektionen och kommit in med handlingar i ärendet.

1.1 Ärendets avgränsning och definitioner

Syftet med Datainspektionens granskning är att kontrollera om nämndens behandling av personuppgifter är förenlig med personuppgiftslagen och om molntjänstleverantörens avtalsvillkor uppfyller personuppgiftslagens krav i förhållande till nämndens personuppgiftsbehandling.

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

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

Personuppgiftsbiträden som är underleverantörer till molntjänstleverantören benämns underleverantörer eller underentreprenörer.

1.2 *Allmänt om nämndens användning av molntjänsten*

Nämnden har i huvudsak anfört följande.

Malmö Stads implementering av molntjänsten benämns Malmö Apps (härefter MaApps). MaApps används sedan hösten 2013 i samtliga kommunala grund-, gymnasie- vuxen- och kulturskolor. Sammanlagt uppgår antalet slutanvändare till cirka 50 000 stycken.

Nämnden använder följande tjänster i MaApps.

- Grupper – en funktion för att skapa grupper för kommunicering och dokumentdelning.
- Drive – en funktion för att dela dokument mellan lärare och elever.
- Sites – en funktion för att skapa webbsidor.
- E-post – varje anställd och elev har ett e-postkonto. Anställdas konton är emellertid begränsade på så sätt att de inte kan skicka eller ta emot extern e-post via MaApps-adressen.
- Google+ - en funktion som användas för kunskapsdelning i olika nätverk. Tjänsten används inte av grundskoleelever.

1.3 *Avtalsförhållandet med molntjänstleverantören*

Nämnden har tecknat följande avtal med molntjänstleverantören.

1. Google Apps for Education Agreement (standardavtal).
2. Data Processing Amendment to Google Apps Enterprise Agreement (personuppgiftsbiträdesavtal).
3. Standard Contractual Clauses (EU-kommissionens standardavtalsklausuler för överföring av personuppgifter till tredje land (2010/87/EU).

Samtliga avtal har tecknats med Google Ireland Limited förutom standardavtalsklausulerna som nämnden har tecknat med Google Inc. i USA.

2 Skäl för beslutet och bedömning

Datainspektionen kommer först ta ställning till om nämndens behandling av personuppgifter i molntjänsten är förenlig med personuppgiftslagen. Därefter följer en bedömning om nämndens instruktioner till biträdet och möjlighet att kontrollera underleverantörer uppfyller kraven i personuppgiftslagen.

2.1 Nämndens behandling av personuppgifter i molntjänsten

Nämnden har anfört i huvudsak följande om sin behandling av personuppgifter i molntjänsten.

Ändamålen med behandlingen av personuppgifter i MaApps är att möjliggöra pedagogiska processer och kommunikation mellan elever och skolpersonal. Personuppgiftsbehandlingen i MaApps utförs i såväl strukturerat som ostrukturerat material (5 a § personuppgiftslagen). För att skapa användarkonton i molntjänsten genereras kontouppgifter automatiskt från nämndens elevadministrativa system Extens. Uppgifterna som används är för- och efternamn, användarnamn och skoltillhörighet. Behandling av andra personuppgifter kan förekomma i exempelvis fritext vid användning av tjänsten.

För att förhindra att känsliga personuppgifter enligt 13 § personuppgiftslagen eller integritetskänsliga personuppgifter, exempelvis uppgifter som omfattas av sekretess eller som rör lagöverträdelser, behandlas i tjänsten har nämnden tagit fram en policy för användandet av MaApps. Policyn är främst riktad till anställda men innehållet ska även kommuniceras ut till eleverna. Ytterst är det rektorn på varje skola som ansvarar för att samtliga användare har tagit del av policyn.

När en anställd avslutar sin tjänst raderar nämnden personen som användare i MaApps efter 45 dagar. När en elev avslutat sin utbildning flyttas dennes användarkonto till ”inaktiva användare” efter 120 dagar. Efter ytterligare 90 dagar raderar nämnden slutligt elevens konto.

Nämnden har tagit fram skriftlig information till vårdnadshavare och elever om behandlingen av personuppgifter i MaApps. Av informationen framgår bland annat att

- nämnden är personuppgiftsansvarig för behandlingen av personuppgifter i MaApps,
- personuppgifter behandlas i syfte att administrera och arbeta i utbildningsverktyget och att uppgifterna inte behandlas i några andra syften, samt
- att eleven och vårdnadshavaren har rätt att begära registerutdrag och rättelse av felaktiga personuppgifter enligt personuppgiftslagen.

2.1.1 Säkerhetsåtgärder

Nämnden uppger att vad som framkommer av dokumenten

- Övergripande systeminformation,
- Policy för användande av MaApps, samt
- de skriftliga bedömningarna av de juridiska förutsättningarna för Malmö stads skolor att använda Google Apps for Education,

ger den samlade bilden av nämndens risk- och sårbarhetsanalys.

Det finns tre olika behörighetsnivåer i MaApps. Utöver den vanliga slutanvändaren finns även behörighet som superadmin och skoladmin. Superadmin kan byta lösenord åt användare, ta emot information från molntjänstleverantören, genomföra kontroller av användarkonton och kontrollera från vilket IP-nummer en viss aktivitet har utförts i molntjänsten. Fyra personer har superadminbehörighet via ett gemensamt konto. Med skoladminbehörighet följer bland annat rätten att skapa grupper och byta lösenord åt användare. Det finns ett skoladminkonto per skolenhet men flera personer kan ha tillgång till kontot. Alla aktiviteter som utförs med ett adminkonto loggas.

2.1.2 Lagtext m.m.

Endast den lagtext som är relevant för beslutet refereras.

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 personuppgifterna är.

Av Datainspektionens Allmänna råd Säkerhet för personuppgifter framgår bland annat följande rörande behörigheter i IT-system (s. 21).

För att förhindra obehörig användning eller åtkomst bör ett system för behörighetskontroll upprättas. Ett sådant system bör omfatta möjligheter att identifiera användare och bekräfta användarens identitet, exempelvis genom användning av personliga lösenord.

2.1.3 Datainspektionens bedömning

Datainspektionen förutsätter att nämnden tar fram individuella användaruppgifter till samtliga användare med behörighet till superadmin- och skoladminkonton.

Datainspektionen konstaterar att nämndens rutiner för behörighetsstyrning av superadmin- och skoladminkonton är otillräckliga eftersom användare loggar in med gemensamma användaruppgifter. Vid utredning av otillåten behandling av personuppgifter i systemen måste en användare kunna identifieras. En förutsättning för att den personuppgiftsansvarige på ett tillfredsställande sätt ska kunna kontrollera vem som har utfört en åtgärd i ett IT-system är att varje användare har individuella användaruppgifter.

Datainspektionen har i övrigt inga synpunkter på vad som framkommit om nämndens personuppgiftsbehandling i molntjänsten. Inspektionen vill framföra att det är positivt att nämnden har gjort en grundlig förstudie och riskanalys innan molntjänsten togs i bruk. Nämnden har också på ett föredömligt sätt genomfört ett flertal laglighetsprövningar såväl innan tjänsten infördes som under dess användning.

2.2 Allmänt om molntjänster

Artikel 29-gruppen[1] har tagit fram ett yttrande om molntjänster[2]. I yttrandet analyseras alla relevanta frågor som rör molntjänstleverantörer som bedriver verksamhet inom EES-området och deras kunder. Yttrandet innehåller även rekommendationer och riktlinjer som är vägledande för samtliga medlemsländer inom EU. I följande del av beslutet har Artikel 29-gruppens rekommendationer och riktlinjer varit vägledande för Datainspektionen.

[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

2.3 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.

2.4 Instruktioner till biträdet – Ändamålen med behandlingen

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.

2.4.1 Lagtext m.m.

Bestämmelser om den personuppgiftsansvariges instruktioner till biträdet finns i 30 § personuppgiftslagen (se ovan under punkten 2.3).

2.4.2 Avtal och yttranden m.m.

Nämndens ändamål med behandling av personuppgifter i MaApps är att möjliggöra pedagogiska processer och kommunikation mellan elever och skolpersonal. Av informationen till de registrerade och deras vårdnadshavare framgår att de personuppgifter som hanteras i MaApps är namn, användarnamn och skoltillhörighet samt att uppgifterna behandlas i syfte att administrera och arbeta i utbildningsverktyget och att uppgifterna inte används eller behandlas i några andra syften.

Av punkten 5.2 Scope of Processing, i biträdesavtalet framgår att kunden, dvs. nämnden, instruerar Google att behandla personuppgifter för följande ändamål.

(a) to comply with Instructions,
(b) to provide the Services (as selected by the Customer via the Admin Console);
(c) to provide product features to facilitate Customer's use of Services and tools for the Customer to create content;
(d) to operate, maintain and support the infrastructure used to provide the Services; and
(e) to respond to customer support requests. Google will only process Customer Data in accordance with this Agreement and will not process Customer Data for any other purpose.

Nämnden har anfört att de ändamål som anges i biträdesavtalet överensstämmer med nämndens egna ändamål för behandling av personuppgifter dvs. att möjliggöra pedagogiska processer och kommunikation mellan lärare och elever. Vid inspektionstillfället uppgav nämnden att biträdet har gjort ändringar i villkorsformuleringen avseende ändamålen för behandling. Ändringarna har dock inte föranletts av att biträdet vidtagit några faktiska förändringar i sin behandling av de personuppgifter nämnden ansvarar för.

2.4.3 Datainspektionens bedömning

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

Utgångspunkten i förhållandet mellan den personuppgiftsansvarige och dennes personuppgiftsbiträde är att biträdet inte har rätt att behandla den ansvariges uppgifter för egna ändamål. När förhållandet mellan en personuppgiftsansvarig och dennes biträde regleras av ett standardavtal är det av avgörande vikt att avtalsvillkoren är tydliga, uttömmande och inte lämnar öppet för olika tolkningsalternativ. Avtalsvillkoren sätter på så sätt ramen för den behandling som biträdet tillåts utföra för den ansvariges räkning.

Enligt Datainspektionens bedömning är nämndens instruktioner till biträdet avseende ändamålen för behandling alltför vida och lämnar utrymme för biträdet att behandla personuppgifter för egna ändamål. Detta gäller särskilt punkten 5.2 (c) som enligt inspektionens uppfattning är både otydlig och svårbegriplig. Oavsett hur ett avtalsvillkor är formulerat vill dock Datainspektionen betona att det är biträdets faktiska behandling av nämndens personuppgifter som är slutligt avgörande för inspektionens bedömning.

2.5 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.

2.5.1 Lagtext m.m.

Bestämmelser om den personuppgiftsansvariges instruktioner till biträdet finns i 30 § personuppgiftslagen (se ovan under punkten 2.3).

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.

2.5.2 Avtal och yttranden

Av punkten 7 i biträdesavtalet framgår följande.

Once Customer or End User deletes Customer Data (and such Customer Data cannot be recovered by the Customer or End User, such as from the "trash") Google will delete such Customer Data (the "Customer-Deleted Data") from its systems as soon as reasonably practicable and within a maximum period of 180 days.

Av punkten 11.4 (iii) i standardavtalet framgår följande rörande radering efter avtalets upphörande.

…after a commercially reasonable period of time, Google will delete Customer Data…

Nämnden har i yttrande den 25 mars 2014 anfört att Malmö stad inte avser att lämna kvar uppgifter om användare, eller uppgifter som lagts in av användarna, i tjänsten efter dess upphörande.

2.5.3 Datainspektionens bedömning

Datainspektionen bedömer att nämndens instruktioner om radering av personuppgifter i personuppgiftsbiträdesavtalet ger tillräckliga garantier för att personuppgiftsbiträdet raderar personuppgifterna inom en rimlig tidsperiod under den tid avtalet löper. Datainspektionen bedömer vidare att nämnden har vidtagit rimliga åtgärder för att säkra att personuppgifter raderas vid avtalets upphörande.

2.6 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.

2.6.1 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 person-

uppgiftsansvarige 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 (här nämnden) 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)).

2.6.2 Avtal och yttranden

Av avsnitt 11 i personuppgiftsbiträdesavtalet framgår att kunden, dvs. nämnden, samtycker till att Google anlitar underleverantörer för att behandla personuppgifter.

Nämnden har inkommit med en utskrift av en webbsida vari Google redogör för de underleverantörer som behandlar personuppgifter. Listan, som är senast uppdaterad den 7 januari 2013, innehåller firmanamn på totalt sex underleverantörer.

Av punkten 11.4 i biträdesavtalet framgår följande avseende information om de underleverantörer som anlitas.

At the written request of the Customer, Google will provide additional information regarding Third Party Suppliers and their locations.

2.6.3 Datainspektionens bedömning

Datainspektionen förutsätter att nämnden kan få omedelbar tillgång till information om personuppgiftsbiträdets samtliga underleverantörer, var de är lokaliserade och vilken typ av uppdrag de utför.

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 personuppgiftsbiträdet tillhandahålla information om vilka bolag som är underleverantörer, var de är lokaliserade och deras huvudsakliga uppgift. Sådan information är avgörande för transparensen i avtalsförhållandet.

Datainspektionen kan konstatera att den information om underleverantörer som personuppgiftsbiträdet tillhandahåller via den aktuella webbsidan inte är tillräcklig. Det saknas information om var bolagen är lokaliserade och vilken typ av uppdrag de utför. Under förutsättning att biträdets egna koncernbolag behandlar personuppgifter saknas även information om var dessa är lokaliserade. Avsaknaden av information reducerar nämndens direkta insyn i biträdets personuppgiftsbehandling. 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.

Datainspektionen vill särskilt betona vikten av att den personuppgiftsansvarige har faktisk möjlighet att utöva kontroll över biträdet och dess underleverantörers behandling av personuppgifter. Det är den personuppgiftsansvariges skyldighet gentemot de registrerade, dvs. anställda och elever, att säkerställa att behandlingen av deras personuppgifter är förenlig med personuppgiftslagen. Datainspektionen förutsätter därför att nämnden har rutiner för att regelbundet kontrollera vilka underleverantörer som anlitas av biträdet.

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 tf enhetschefen Anna Hörnlund efter föredragning av juristen Ingela Alverfors. Vid handläggningen av ärendet har även IT-säkerhetsspecialisten Fredrik Ekman deltagit.

Anna Hörnlund

Ingela Alverfors

Kopia till:
Personuppgiftsombudet