Datainspektionen

Datum
2013-09-09

Diarienr
890-2012

Utbildnings- och
arbetsmarknadsnämnden
Sollentuna kommun
Turebergs torg 1
191 86 Sollentuna

Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av personuppgifter i molnet

Datainspektionens beslut

Datainspektionen förelägger Utbildnings- och arbetsmarknadsnämnden i Sollentuna kommun att vidta åtgärder för att antingen teckna ett personuppgiftsbiträdesavtal som uppfyller bestämmelserna i personuppgiftslagen med molntjänstleverantören eller att upphöra med sin behandling av personuppgifter i molntjänsten.

Ärendet avslutas men kan komma att följas upp.

Redogörelse för tillsynsärendet

Rudbecksskolan är en kommunal gymnasieskola i Sollentuna kommun. På skolan är knappt 2 000 elever inskrivna och det finns ca 200 anställda.

Genom ett klagomål har Datainspektionen uppmärksammats på att Rudbecksskolan använder molntjänsten Google Apps for Education i sin verksamhet. Enligt klagomålet måste samtliga lärare och elever öppna ett konto hos molntjänstleverantören för att få tillgång till de verktyg som behövs för skolarbetet.

Med anledning av det inkomna klagomålet beslutade Datainspektionen att inleda tillsyn mot Utbildnings- och arbetsmarknadsnämnden i Sollentuna kommun (nämnden). Nämnden har inledningsvis besvarat ett antal frågor skriftligen. I januari 2013 genomfördes också en inspektion på plats i Rudbecksskolan. Nämnden har yttrat sig över protokollet från inspektionen och kommit in med följande kompletterande handlingar.

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 mellan Sollentuna kommun och molntjänstleverantören (Google Apps Education Edition Agreement).
- Riktlinjer till elever för skol- eller hyrdator.
- Risk- och sårbarhetsanalys.
- Riktlinjer kring post och e-post.

Nämndens behandling av personuppgifter
Under ärendets handläggning och vid inspektionen på plats har följande framkommit om nämndens behandling av personuppgifter i molntjänsten.

Google Apps for Education introducerades år 2010 på Rudbecksskolan. I dagsläget används tjänsterna e-post, kalender, Drive och Sites. Tjänsterna används som en gemensam lär- och samarbetsplattform där elever och lärare kan kommunicera både enskilt och öppet, arbeta med gemensamma dokument m.m. Vissa lärare arbetar mycket aktivt med molntjänsten och skapar nya användningsområden. Andra lärare använder i princip inte tjänsterna alls.

Samtliga lärare och elever har varsitt konto för att komma åt tjänsterna. Ett konto registreras med hjälp av namn och skoltillhörighet.

På uppdrag av Barn- och utbildningskontoret i Sollentuna kommun har under år 2012 en risk- och sårbarhetsanalys genomförts rörande användningen av molntjänsten.

Nämnden har inte tagit fram några instruktioner eller riktlinjer som är särskit avsedda för hanteringen av personuppgifter i molntjänsten. Av riktlinjerna till anställda kring post och e-posthantering framgår att handlingar som omfattas av sekretess eller känsliga personuppgifter enligt PuL inte ska skickas via e-post, fax, SMS eller liknande. Av riktlinjerna till elever för skol- och hyrdator framgår bland annat (punkten 3.4) att eleven ska visa respekt för andra människor och att eleven inte får sprida texter, bilder eller ljud som kan upplevas som kränkande eller nedsättande.

Nämnden har inte upprättat något specifikt personuppgiftsbiträdesavtal med molntjänstleverantören.

Allmänt om behandling av personuppgifter i molnet
Enligt vad Datainspektionen erfar har det blivit allt vanligare att utbildningsverksamheter använder olika typer av molntjänster där anställda och elevers personuppgifter behandlas. I vissa fall kan det till och med vara en förutsättning att såväl anställda som elever skapar konton i molnet för att kunna medverka och tillgodogöra sig undervisningen.

Datainspektionen har förståelse för att det kan finnas fördelar med att använda molntjänster såväl vad avser funktion, effektivitet och ekonomi. Det verkar dock finnas en tendens inom just utbildningsområdet att i viss mån acceptera att de biträdesavtal som erbjuds av molntjänstleverantörerna inte alltid, i alla avseenden uppfyller kraven i PuL. Datainspektionen vill här påminna om att den som har för avsikt att behandla personuppgifter i en molntjänst är skyldig att se till att de avtal som erbjuds eller förhandlas fram uppfyller *samtliga* bestämmelser i PuL eller annan tillämplig integritetsskyddslagstiftning. När det gäller utbildningsverksamheter som rör grundskola och gymnasium ska den personuppgiftsansvarige i synnerhet beakta att behandlingen av personuppgifter rör barn och unga och är därför särskilt skyddsvärd.

Är nämndens behandling strukturerad eller ostrukturerad?
PuL bygger på två olika regelsystem; hanteringsreglerna och missbruksregeln. Vilket system som ska användas beror på hur materialet med personuppgifter är utformat. När personuppgifter exempelvis behandlas i IT-system som är strukturerade på ett sätt som underlättar sökning på personuppgifter, exempelvis ett ärendehanteringssystem eller diarium, gäller hanteringsreglerna. Hanteringsreglerna innebär att samtliga bestämmelser i PuL måste tillämpas.

För behandling av personuppgifter i exempelvis löpande text eller e-postmeddelanden där materialet inte är uppbyggt för att i första hand vara direkt sökbart på personuppgifter gäller missbruksregeln (5 a § PuL). Enligt missbruksregeln är en behandling av personuppgifter tillåten så länge den inte kränker den enskildes personliga integritet. En konsekvens av att missbruksregeln är tillämplig på behandlingen är att flertalet bestämmelser i PuL inte behöver följas. Säkerhetsbestämmelserna i 31 § PuL och kravet på personuppgiftsbiträdesavtal i 30 § PuL gäller dock alltid.

Datainspektionen har inte närmare utrett vilket material som är strukturerat respektive ostrukturerat i nämndens personuppgiftsbehandling. Inspektionen förutsätter dock att nämnden behandlar personuppgifter i såväl strukturerat som i ostrukturerat material i molntjänsten.

Kravet på personuppgiftsbiträdesavtal
Oavsett om nämndens personuppgiftsbehandling är strukturerad eller ostrukturerad är nämnden skyldig att teckna ett personuppgiftsbiträdesavtal med molntjänstleverantören (30 § PuL). I ett sådant avtal ska det särskilt föreskrivas att biträdet dvs. molntjänstleverantören, får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige

dvs. nämnden, 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. Bland annat måste instruktionerna omfatta ändamålet med behandlingen och reglera hur länge uppgifterna får bevaras hos biträdet.

Nämnden har inte tecknat ett specifikt personuppgiftsbiträdes avtal med molntjänstleverantören. I avtalet som har tecknats mellan parterna saknas bland annat instruktioner till biträdet om för vilka ändamål denne får behandla nämndens personuppgifter, hur länge biträdet får bevara uppgifterna samt vilka säkerhetsåtgärder biträdet är skyldigt att vidta.

Överföring till tredje land och underleverantörer
Enligt huvudregeln i PuL (33 §) är det förbjudet att föra över personuppgifter till tredje land om inte landet har en adekvat nivå för skyddet av personuppgifterna.

Av avtalet som tecknats mellan parterna (punkten 1.7) framgår att molntjänstleverantören kan komma att lagra och bearbeta personuppgifter i USA eller i något annat land där molntjänstleverantören eller någon av dess representanter har lokaler.

I avtalet mellan parterna framgår inte om det finns någon tillåtlig grund för att överföra personuppgifter till tredje land. Det saknas också reglering om under vilka förhållanden molntjänstleverantören får anlita underleverantörer.

Skäl för beslutet
Nämnden är personuppgiftsansvarig för elever och anställdas behandling av personuppgifter i molntjänsten. Molntjänstleverantören behandlar personuppgifter på uppdrag av nämnden och är därmed nämndens personuppgiftsbiträde.

Nämnden har inte tecknat ett personuppgiftsbiträdesavtal med molntjänstleverantören. I avtalet som har tecknats mellan parterna saknas bland annat instruktioner och begränsningar för molntjänstleverantörens personuppgiftsbehandling. Det finns inte heller angivet vilka säkerhetsåtgärder molntjänstleverantören är skyldigt att vidta för att skydda personuppgifterna som behandlas. I avtalet regleras inte heller vilken tillåtlig grund som används för att överföra personuppgifter till tredje land eller att molntjänstleverantören överhuvudtaget har rätt att anlita underleverantörer för behandlingen av nämndens personuppgifter.

Mot bakgrund av ovanstående föreläggs nämnden att snarast teckna ett personuppgiftsbiträdesavtal som lever upp till reglerna i PuL med molntjänstleverantören eller att upphöra med behandlingen av personuppgifter i molntjänsten.

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.

Ingela Alverfors

Kopia till:
Personuppgiftsombudet