



Beslut
2008-09-09

Dnr
1310-2007

Bildningsnämnden
Upplands-Bro kommun
196 81 Kungsängen

Beslut efter tillsyn enligt personuppgiftslagen (1998:204) – PuL

Datainspektionens beslut

Datainspektionen konstaterar att Bildningsnämnden i Upplands-Bro kommun (härefter nämnden):

1. behandlar personuppgifter i fritextfältet i Skola24 i strid med kravet i 9 § PuL på särskilda, uttryckligt angivna och berättigade ändamål
2. behandlar känsliga personuppgifter i fritextfältet i Skola24 i strid med kravet i 15 § PuL på samtycke
3. behandlar känsliga och andra integritetskänsliga personuppgifter utan att vidta tillräckliga säkerhetsåtgärder enligt 31 § PuL
4. behandlar personuppgifter i strid med kravet i 30 § PuL på personuppgiftsbiträdesavtal
5. behandlar personuppgifter i strid med kravet i 9 § punkten i) PuL att personuppgifter inte ska bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Datainspektionen förutsätter att nämnden:

1. utfärdar skriftliga instruktioner till användarna om vilka uppgifter som är relevanta att lämna i fritextfältet i Skola24
2. inhämtar samtycke till behandlingen av känsliga personuppgifter i fritextfältet i Skola24
3. vidtar tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifterna i Skola24
4. ingår personuppgiftsbiträdesavtal med sina personuppgiftsbiträden
5. tar fram riktlinjer och rutiner för gallring av personuppgifter i Skola24.

Ärendet avslutas men kan komma att följas upp.

Bakgrund

Datainspektionen fick i oktober 2007 in ett klagomål på nämndens personuppgiftsbehandling i Skola24, bl.a. angående samtycke till behandling av

känsliga personuppgifter och noteringar i det för frånvarorapportering avsedda fritextfältet.

Med anledning av klagomålet inledde Datainspektionen tillsyn mot nämnden och genomförde inom ramen för tillsynen en inspektion i Hagnässkolan den 11 februari 2008.

Under tillsynen har bl.a. följande framkommit.

Det finns ett fritextfält i Skola24 som av nämnden används för att rapportera bl.a. om elever är frånvarande pga. sjukdom, om de betar sig olämpligt och för att framföra andra meddelande av olika slag till vårdnadshavarna, exempelvis meddelanden om hur elever bör vara klädda inför vissa skolaktiviteter. Nämnden har inga skriftliga riktlinjer för vad som får skrivas in i fritextfältet. Det har förekommit att lärare i fritextfältet har återgivit grova glåpord som vissa elever enligt lärarna har yttrat i skolan.

På en särskild samtyckesblankett kan vårdnadshavare lämna samtycke till nämnden för behandling i Skola24 av följande uppgifter: Elevens namn och klass samt vårdnadshavarens namn, personnummer och e-postadress.

Tekniskt underhåll och drift av nämndens elevadministrativa system sköts av utomstående företag som är personuppgiftsbiträden i förhållande till nämnden. Nämnden har inga personuppgiftsbiträdesavtal med företagen.

Användarna har åtkomst till Skola24 över Internet. Inloggning i Skola24 på Internet sker med användarnamn och lösenord.

Elevernas frånvarohistorik raderas när eleven går ut grundskolan. Nämnden har ingen kännedom om när och hur gallring av personuppgifter sker hos de företag som är personuppgiftsbiträden.

Datainspektionens bedömning

- Personuppgifter i fritextfält

I PuL finns bestämmelser om grundläggande krav på behandlingen av personuppgifter. I 9 § punkten c) PuL anges följande:

Den personuppgiftsansvarige skall se till att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål.

Bestämmelsen innebär att ändamålen måste bestämmas redan när uppgifterna samlas in och att ändamålen måste ha en viss precision. Detta innebär enligt Datainspektionens mening att det i regel krävs *skriftliga* instruktioner till användarna om vilka uppgifter som är relevanta att lämna i ett fritextfält (se Datainspektionens beslut den 14 februari 2007, dnr 1623-2006). Instruktionerna bör exempelvis ange hur värderande omdömen om eleven ska formuleras och att kränkande uttalanden inte är tillåtna.

I ärendet har emellertid framkommit att användandet av fritextfältet i Skola24 inte är begränsat till några särskilda och uttryckligt angivna ändamål. Exempelvis används fritextfältet både för att kommunicera meddelanden om hur elever bör vara klädda inför vissa skolaktiviteter, och för att återge glåpor som vissa elever enligt lärarna har yttrat i skolan. Nämnden har inte heller några skriftliga riktlinjer för vad som får skrivas in i fritextfältet.

Om nämnden vill fortsätta att behandla personuppgifter i fritextfältet i Skola24, förutsätter Datainspektionen att nämnden utfärdar skriftliga instruktioner till användarna om vilka uppgifter som är relevanta att lämna i fritextfältet.

- Känsliga personuppgifter

13 § PuL innehåller följande förbud mot att behandla känsliga personuppgifter.

Det är förbjudet att behandla personuppgifter som avslöjar

- a) ras eller etniskt ursprung,*
- b) politiska åsikter,*
- c) religiös eller filosofisk övertygelse, eller*
- d) medlemskap i fackförening.*

Det är också förbjudet att behandla sådana personuppgifter som rör hälsa eller sexualliv.

Uppgifter av den art som anges i första och andra styckena betecknas i denna lag som känsliga personuppgifter.

15 § PuL innehåller följande bestämmelse om behandling av känsliga personuppgifter.

Känsliga personuppgifter får behandlas, om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt offentliggjort uppgifterna.

I 16-19 §§ PuL finns bestämmelser som anger när känsliga personuppgifter får behandlas även utan uttryckligt samtycke eller eget offentliggörande.

Datainspektionen anser att ingen av dessa bestämmelser, och inte heller någon undantagsbestämmelse i annan författning, kan tillämpas i ärendet.

En uppgift om att en elev är sjuk är, alldeles oavsett om symtom eller diagnos anges, en känslig personuppgift i personuppgiftslagens mening.

I ärendet har framkommit att det kan förekomma att uppgifter om sjukdom behandlas i fritextfältet i Skola24, utan att nämnden inhämtar uttryckligt samtycke till behandling av känsliga personuppgifter.

Om nämnden vill fortsätta att behandla känsliga personuppgifter i fritextfältet i Skola24, förutsätter Datainspektionen att nämnden inhämtar samtycke till sådan behandling.

- Säkerhetsåtgärder

I PuL finns bestämmelser om säkerhetsåtgärder. I lagens 31 § första stycket anges följande.

Den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall 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.*

Enligt Datainspektionen innebär bestämmelsen att känsliga personuppgifter enligt PuL eller andra personuppgifter som kan anses vara integritetskänsliga, t.ex. för att de omfattas av sekretess eller rör den enskildes personliga förhållanden, får lämnas ut via Internet endast till identifierade användare vars identitet är säkerställd med en teknisk funktion som asymmetrisk kryptering, exempelvis e-legitimation, engångslösenord eller motsvarande.

I ärendet har framkommit att nämnden i Skola24 behandlar känsliga och andra integritetskänsliga uppgifter; dessa kan vara är uppgifter om sjukdom, frånvaro, besök hos skolhälsovården och uppgifter om elevernas uppförande. Vidare har framkommit att användarna har åtkomst till Skola24 över Internet och att Internetinloggning i Skola24 sker med endast användarnamn och lösenord.

Behandlingen av personuppgifter i Skola24 uppfyller därmed inte säkerhetskraven i PuL beträffande känsliga och andra integritetskänsliga personuppgifter.

Om nämnden vill fortsätta att behandla uppgifter av detta slag i Skola24 och ge åtkomst till uppgifterna över Internet, förutsätter Datainspektionen att nämnden vidtar tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifterna i Skola24 (dvs. att nämnden börjar använda sig av asymmetrisk kryptering, exempelvis e-legitimation, engångslösenord eller motsvarande).

- Personuppgiftsbiträdesavtal

I PuL finns bestämmelser om avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet. I lagens 30 § andra stycket anges följande.

Det skall finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet skall 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.

Vidare anges i 31 § andra stycket PuL följande.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, skall den personuppgiftsansvarige förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

I ärendet har framkommit att tekniskt underhåll och drift av nämndens elevadministrativa system sköts av utomstående och att nämnden saknar personuppgiftsbiträdesavtal med företagen.

Datainspektionen förutsätter att nämnden ingår sådana avtal med sina personuppgiftsbiträden.

- Bevarande och gallring

I PuL finns bestämmelser om grundläggande kraven på behandlingen av personuppgifter. I 9 § punkten i) PuL anges följande:

Den personuppgiftsansvarige skall se till att personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Bestämmelsen ska dock bara tillämpas i den mån det inte i annan lag eller förordning finns avvikande bestämmelser. Detta framgår bl.a. av 8 § andra stycket första meningen PuL, där följande anges.

Bestämmelserna hindrar inte heller att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.

I ärendet har framkommit att nämnden saknar riktlinjer och rutiner för bevarande och gallring av personuppgifter i Skola24.

Datainspektionen förutsätter därför att nämnden tar fram riktlinjer och rutiner för bevarande och gallring av personuppgifter, vilka även omfattar de handlingar som personuppgiftsbiträdena utför på nämndens uppdrag.

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 Länsrätten i Stockholms län för prövning om inspektionen inte själv ändrar beslutet på det sätt Ni har begärt.

Erik Janzon

Kopia till:

Personuppgiftsombudet Jan Näsmark
Bildningsförvaltningen, Administrativa avdelningen
Upplands-Bro kommun
196 81 Kungsängen

Klaganden