Bilaga 1

Datainspektionen

Datum	Diarienr
2009-12-11	1344-2009

Utbildningsnämnden i Stockholms stad
Box 22049
104 22 Stockholm

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

Datainspektionens beslut

Datainspektionen konstaterar att Utbildningsnämnden i Stockholms stad (härefter Utbildningsnämnden):
1. behandlar personuppgifter i Hanna i strid med kravet i 31 § PuL på att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder
2. behandlar personuppgifter i fritextfälten i Fronter i strid med kravet i 9 § PuL på särskilda, uttryckligt angivna och berättigade ändamål
3.behandlar personuppgifter i strid med kravet i 9 § punkten i) PuL att personuppgifter inte skall bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Datainspektionen förutsätter att Utbildningsnämnden vidtar följande åtgärder.
1. Vidtar lämpliga tekniska och organisatoriska åtgärder så att användarnas behörighet i Hanna på ett bättre sätt anpassas till användarnas behov av tillgång till uppgifter för att kunna utföra sitt arbete.
2. Utfärdar skriftliga instruktioner till användarna om vilka uppgifter som är relevanta att lämna i fritextfälten i Fronter.
3. Senast den 30 april 2010 inkommer till Datainspektionen med en redogörelse för hur arbetet med att ta fram rutiner och riktlinjer för bevarande och gallring av personuppgifter i Fronter har omhändertagits.

Ärendet avslutas men kan komma att följas upp.

Bakgrund

Datainspektionen genomförde den 12 oktober 2009 en inspektion av Utbildningsnämndens personuppgiftsbehandling på Norra Real.

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

Under inspektionen och i efterföljande skriftväxling, har bl.a. följande framkommit.

De IT-stöd som används på Norra Real och som innehåller personuppgifter om elever, och i förekommande fall vårdnadshavare, är bl.a. Hanna och Fronter. Det finns ett edu-nät och ett administrativt nät.

Hanna
Hanna är nämndens centrala system för registrering av de elever som går i gymnasieskolor i Stockholms stad. Systemet innehåller elevernas namn, personnummer, adress, telefonnummer, e-post, skola, betyg, betygsliknande omdömen, studieplan, studieväg, klass- och grupptillhörighet, antal frånvarotimmar (skrivs ut på betyg), anhöriglistor, tillfälliga aktivitetslistor, rapportering till CSN, elevnotering. För elevernas vårdnadshavare finns uppgift om namn, personnummer, adress, telefonnummer och e-post.

På skolan har kanslister, skolledare, studie- och yrkesvägledare, elevvårdspersonal och lärare behörighet till Hanna. Behörighetsprofilen ser olika ut för olika kategorier. Lärarna har åtkomst till uppgifter rörande skolans elever. De som varit, men slutat som, lärare även på andra skolor i Stockholms stad har åtkomst till viss information även om de elever som ingick i respektive lärares kursgrupp vid tidigare skola.

Alla användare i Hanna kan med hjälp av sökning på personnummer ta del av viss information om vilken elev som helst i vilken som helst av Stockholms stads gymnasieskolor. När sökning sker på elevs personnummer ges åtkomst till uppgift om elevens namn, skola, klass, individuell studieplan, betyg och omdöme. Någon skrivbehörighet för elever vid andra skolor finns inte. Enligt Utbildningsnämnden kan läraren ibland, t.ex. när en elev flyttar över från en annan skola, behöva ta del av elevers uppgifter från andra skolor. Utbildningsnämnden uppger vidare att det i Hanna är tekniskt sett relativt komplicerat att begränsa lärarnas behörighet så att de vid sökning på personnummer inte får åtkomst till information om elever vid andra skolor. Mot bakgrund av detta samt att det handlar om uppgifter som vid begäran enligt offentlighetsprincipen skulle ha lämnats ut och att det är osannolikt att lärare skulle söka fram uppgifterna om de inte behövs, har Utbildningsnämnden bedömt att behovet av ytterligare behörighetsbegränsningar inte motiverar de kostnader som är förenligt med detta.

För drift av Hanna har nämnden anlitat Tieto. Personuppgiftsbiträdesavtal finns.

Gallring av uppgifter i Hanna sker enligt gallringsplan, vilken för närvarande anger att uppgifter skall gallras efter 8 år (i vissa fall tidigare). Arbete med eventuella justeringar av gallringsplanen pågår.

Fronter
Fronter är skolans lärplattform, d.v.s. system för administration och kommunikation. Systemet är uppdelat på ett stort antal webbaserade ”rum” för lärare och elever. I dessa rum kan det ske undervisning i kursgrupper, diskussioner mellan deltagare, inlämning av uppgifter, förmedling av nyheter m.m. Det är lärarna som har behörighet att skapa nya rum, kontrollera informationen och vid behov ta bort uppgifter.

I anslutning till kursgruppernas rum finns en funktion (portfolio) som gör det möjligt för lärarna att genom noteringar i fritextfält kommunicera feedback till varje elev. Det finns inga dokumenterade riktlinjer som anger vad som är relevant, eller inte relevant, att notera i fritextfältet.

De uppgifter som behandlas om eleverna är namn, klass, grupper, personnummer, adress, studieplan (kurser, poäng, betyg), frånvaro, provresultat (kan finnas), omdöme, e-post och telefonnummer. Inom kort kommer även IUP att inkluderas i Fronter.

De uppgifter om frånvaro som finns är ogiltig, giltig och elevregistrerad frånvaro. För lärarna finns även ett fritextfält där kommentarer om frånvaron kan noteras. Det finns inga skriftliga rutiner eller riktlinjer som anger vad som är relevant att notera i fritextfältet.

Elever, lärare/mentor, administratör, skolans superadministratör samt vårdnadshavare har webbåtkomst till Fronter. För elever sker inloggning med användarnamn och lösenord. Lärare och övrig personal loggar in med e-legitimation eller användarnamn, lösenord samt engångslösenord via sms. Vårdnadshavare loggar in med e-legitimation.

Lärarnas behörighet till uppgifter i Fronter styrs av tjänstefördelningen i Hanna, vilket innebär att lärarna endast har åtkomst till uppgifter rörande elever i sin egen undervisning.

Eleverna har åtkomst till uppgifter rörande de webbaserade rum eleven är medlem i.

Vårdnadshavare har åtkomst till sitt barns frånvaro, studieplan, information i och inför elevens individuella val, omdöme, portfolio samt kontaktuppgifter.

Vårdnadshavare har även åtkomst till uppgifter om möten bokade mellan vårdnadshavare och skolan samt vårdnadshavarens egna kontaktuppgifter.

Gallringsbeslut saknas för Fronter. En gallringsutredning med bevarandeplan har påbörjats.

För drift av systemet har nämnden anlitat företaget Fronter. Det finns ett personuppgiftsbiträdesavtal med Fronter.

Samtliga elever och vårdnadshavare informeras om personuppgiftsbehandlingen i skolan. Information sker genom dokumentet ”Behandling av personuppgifter”.

Datainspektionens bedömning

Behörighetsstyrning
Enligt 31 § PuL skall den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Det handlar bl.a. om att se till att personuppgifter endast är åtkomliga för de användare som behöver uppgifter för att exempelvis utföra sitt arbete.

I ärendet har framkommit att användare i Hanna, t.ex. lärare, med hjälp av sökning på personnummer kan ta del av viss information om vilken elev som helst i vilken som helst av Stockholms stads gymnasieskolor. När sökning sker på elevs personnummer ges åtkomst till uppgift om elevens namn, skola, klass, individuell studieplan, betyg och omdöme. Utbildningsnämnden har inte redogjort för att det skulle finnas ett generellt behov av att ta del av uppgifter om elever vid andra skolor. Behovet finns bara när elever byter skola. Vidare har Utbildningsnämnden anfört att det skulle vara tekniskt sett relativt komplicerat att begränsa behörigheten till att avse elever vid den egna skolan samt även att det är fråga om uppgifter som ändå hade lämnats ut vid en begäran enligt offentlighetsprincipen.

Datainspektionen vill i sammanhanget poängtera att offentlighetsprincipens syfte bl.a. är att ge *utomstående* möjlighet att efter begäran ta del av allmänna handlingar, inte att ge myndigheter möjligheten att på eget initiativ tillgängliggöra uppgifter internt inom myndigheten. Den interna tillgången till personuppgifter skall därmed utformas efter användarnas behov av uppgifter för att kunna utföra sitt arbete, inte efter förekomsten av allmänna handlingar.

Vid en samlad bedömning och med hänsyn till det stora antal elever som deltar, eller har deltagit, i undervisning i Stockholms stads gymnasieskolor och det stora antalet användare av Hanna bedömer Datainspektionen att det innebär en obefogad spridning av personuppgifter att ge samtliga användare i Hanna möjlighet att med hjälp av sökning på personnummer ta del av uppgifter om elever vid andra skolor. Datainspektionen förutsätter att Utbildningsnämnden ser över behörighetsstyrningen till Hanna och vidtar lämpliga tekniska och organisatoriska åtgärder så att användarnas behörighet på ett bättre sätt anpassas till användarnas behov av tillgång till uppgifter för att kunna utföra sitt arbete.

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. Instruktionerna bör exempelvis ange hur värderande omdömen om eleven skall formuleras och att kränkande uttalanden inte är tillåtna.

I ärendet har framkommit att Fronter innehåller fritextfält i anslutning till frånvarorapporteringen och portfolion (feedback till eleverna). Vidare har framkommit att Utbildningsnämnden inte har några skriftliga rutiner och instruktioner för dokumentationen i fritextfälten.

Datainspektionen förutsätter att Utbildningsnämnden, om den vill fortsätta att behandla personuppgifter i fritextfälten i Fronter, utfärdar skriftliga instruktioner till användarna om vilka uppgifter som är relevanta att lämna i fritextfälten.

Säkerhetsåtgärder vid åtkomst till personuppgifter över Internet
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."

Bestämmelsen innebär, enligt Datainspektionen, 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.

Känsliga personuppgifter enligt PuL är bl.a. uppgift om hälsa, sexualliv, etniskt ursprung och religiös övertygelse. Som exempel på personuppgifter som kan anses vara integritetskänsliga kan nämnas värderande omdömen om elevers sociala utveckling.

I ärendet har framkommit att personal och vårdnadshavare har åtkomst till Fronter över Internet genom inloggning med e-legitimation eller användarnamn, lösenord samt engångslösenord. Elevernas åtkomst över Internet sker emellertid endast med användarnamn och lösenord. Uppmärksammas skall dock att eleverna i dagsläget inte ges åtkomst till integritetskänsliga personuppgifter.

De redovisade säkerhetsåtgärderna vid behandlingen av personuppgifter i Fronter uppfyller enligt Datainspektionens mening säkerhetskraven i PuL beträffande integritetskänsliga personuppgifter. Samtidigt vill Datainspektionen uppmärksamma Utbildningsnämnden på att en annan bedömning kan vara påkallad för det fall IUP eller annan framtida dokumentation i Fronter kommer att innehålla integritetskänsliga personuppgifter och tillhandahållas eleverna genom åtkomst över Internet.

Bevarande och gallring
I PuL finns bestämmelser om grundläggande krav på behandling 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 skall dock bara tillämpas i den mån det inte i annan lag eller förordning finns avvikande bestämmelser. Detta framgår av 8 § andra stycket första meningen PuL, där följande anges.

> ”Bestämmelsen hindrar inte heller att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas omhand av en arkivmyndighet.”

I ärendet har framkommit att Utbildningsnämnden inte gallrar uppgifter i Fronter, men att en gallringsutredning med bevarandeplan har påbörjats.

Att personuppgifter som inte längre behövs skall gallras är en av hörnstenarna i integritetsskyddslagstiftningen. Att samtliga personuppgifter, som i behandlas i och för elevers skolgång, bevaras för all framtid kan enligt Datainspektionen utgöra ett integritetsintrång. Finns det ingen plan för vilka uppgifter som skall bevaras för framtiden och hur bevarandet skall gå till är det enligt Datainspektionen svårt att hävda att bevarandet är befogat. Datainspektionen ställer sig frågande till om Utbildningsnämnden verkligen har något behov av att spara sådana personuppgifter som inte omfattas av specifika bestämmelser om bevarande eller annars bedöms nödvändiga för att t.ex. tillgodose rätten att ta del av allmänna handlingar, behovet av information för rättskipning och förvaltning eller vetenskapliga ändamål (forskning). I sammanhanget vill Datainspektionen upplysningsvis uppmärksamma Utbildningsnämnden på Riksarkivets allmänna råd (RA-FS 2002:2) om bevarande och gallring av handlingar rörande kommunernas och landstingens utbildningsväsende. I de allmänna råden anges bl.a. vilka handlingar som bör bevaras och vilka som kan gallras. Bland de handlingar som kan gallras nämns exempelvis skriftlig information sammanställd i samband med utvecklingssamtal, rutinkorrespondens, frånvaroregister och handlingar som legat till underlag för frånvaroregistret m.m.

Mot bakgrund av ovanstående förutsätter Datainspektionen att Utbildningsnämnden i sitt fortsatta arbete, på uppgiftsnivå, analyserar och utvärderar behovet av bevarande av uppgifter i Fronter och utifrån detta tar fram riktlinjer och rutiner för bevarande och gallring av personuppgifter. Datainspektionen vill att Utbildningsnämnden senast den 30 april 2010 lämnar in en redogörelse till Datainspektionen för hur arbetet med att ta fram rutiner för bevarande och gallring har omhändertagits. I sammanhanget vill Datainspektionen upplysningsvis informera om vikten av att Utbildningsnämnden även försäkrar sig om att personuppgiftsbiträdet Fronter följer nämndens rutiner för bevarande och gallring.

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.

Beslut i detta ärende har fattats av teamledaren Erik Janzon i närvaro av IT-säkerhetsspecialisterna Magnus Bergström och Adolf Slama samt juristerna Ulrika Harnesk och Patrik Sundström, föredragande.

Erik Janzon

Patrik Sundström

Kopia till:

Per Engback, rektor, Norra Real, Roslagsgatan 1, 113 55 Stockholm

Thomas Persson, förvaltningschef, Utbildningsförvaltningen, Stockholms stad, Box 22049, 104 22 Stockholm

Ylva Larsson, personuppgiftsombud, Utbildningsförvaltningen, Stockholms stad, Box 22049, 104 22 Stockholm