

Barn- och utbildningsnämnden  
Tyresö Kommun  
135 81 Tyresö

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

### **Datainspektionens beslut**

Datainspektionen konstaterar att Barn- och utbildningsnämnden i Tyresö kommun (härefter nämnden):

1. behandlar personuppgifter i fritextfälten i Extens/Skolportalen i strid med kravet i 9 § PuL på särskilda, uttryckligt angivna och berättigade ändamål
2. behandlar känsliga personuppgifter i Extens/Skolportalen i strid med kravet på samtycke i 15 § PuL
3. behandlar känsliga och integritetskänsliga personuppgifter i strid med kravet i 31 § PuL på att vidta tillräckliga säkerhetsåtgärder (autentisering vid åtkomst över Internet)
4. 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
5. behandlar personuppgifter i Extens/Skolportalen utan att informera de registrerade om behandlingen
6. inhämtar samtycke till behandlingen i Extens/Skolportalen utan att det tydligt framgår vad samtycket avser.

Datainspektionen förutsätter att nämnden vidtar följande åtgärder.

1. Utfärdar skriftliga instruktioner till användarna om vilka uppgifter som är relevanta att lämna i fritextfälten i Extens/Skolportalen.
2. Inhämtar samtycke till behandlingen av känsliga personuppgifter i Extens/Skolportalen.
3. Vidtar tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifter i Extens/Skolportalen.
4. Tar fram riktlinjer och rutiner för bevarande och gallring av personuppgifter i Extens/Skolportalen.

5. Ger vårdnadshavarna och eleverna fullständig information om den personuppgiftsbehandling som sker i Extens/Skolportalen
6. Genomför en analys av den samtyckeshantering som sker i samband med inloggning i Extens/Skolportalen.

Senast den 30 april 2010 skall nämnden inkomma med en redogörelse till Datainspektionen för hur påpekandena avseende punkterna 1-6 har omhändertagits och åtgärdats.

Ärendet avslutas men kan komma att följas upp.

### **Bakgrund**

Datainspektionen fick i november 2007 in ett klagomål beträffande nämndens personuppgiftsbehandling i Skolportalen, bl.a. beträffande säkerhetsåtgärder. Med anledning av klagomålet inledde Datainspektionen tillsyn mot nämnden, vilket avslutades med beslut i september 2008 (dnr 31-2008). I beslutet konstaterade Datainspektionen bl.a. att nämnden behandlade integritetskänsliga personuppgifter i strid med 31 § PuL, varvid Datainspektionen förutsatte att nämnden skulle vidta tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifter i Skolportalen.

Inom ramen för ett uppföljande tillsynsprojekt genomförde Datainspektionen den 5 oktober 2009 en inspektion av nämndens personuppgiftsbehandling på Tyresö skola.

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

De IT-stöd som används på Tyresö skola och som innehåller personuppgifter om elever, och i förekommande fall vårdnadshavare, är bl.a. Novell och Extens/Skolportalen. Det finns ett edu-nät och ett administrativt nät. All systemdrift sker redundantly i kommunens egen regi.

#### *Novell*

Novell är ett system på det administrativa nätverket som används centralt på Tyresö kommuns IT-avdelning för registrering av elever. Systemet innehåller uppgift om elevernas namn, personnummer, skola, klass och vårdnadshavare. Det innehåller även uppgift om användarnamn och lösenord (ej klartext). Genom systemet skapas elevers e-postkonton och användaruppgifter.

### *Extens/Skolportalen*

I databasen Extens behandlas uppgifter om elevernas namn, personnummer, adress, telefonnummer, betyg, schema, frånvaro, skolval, ämnesval, klass, studieplan, lärare, modersmål, IUP, uppgifter inför utvecklingssamtal, resultat i nationellt ämnesprov, vårdnadshavare, vårdnadshavares telefonnummer och inkomstuppgifter (barnomsorg), elevers och vårdnadshavares e-post, uppgift (namn, personnummer, adress) om samtliga familjemedlemmar som är folkbokförda i kommunen.

Skolportalen är ett webbaserat gränssnitt som medger åtkomst till uppgifter i Extens.

Elevers frånvaro kan registreras genom att välja fasta frånvaroorsaker, exempelvis sjukdom elev, vård av barn, beviljad ledighet, avvikit från lektion, frånvarande av okänd orsak och frånvarande av känd orsak. Det finns inget fritextfält i samband med frånvaroregistreringen. Det inhämtas inget samtycke till frånvaroregistreringen.

Det finns ett antal fritextfält i samband med dokumentationen inför ett utvecklingssamtal och framtagande av utvecklingsmål. Inför utvecklingssamtal får elevernas vårdnadshavare elektroniskt svara på ett antal frågor som sedan registreras i systemet. Svar på frågorna kan lämnas dels genom att välja fyra alternativ från ”stämmer mindre bra” till ”stämmer mycket bra”. I anslutning till frågorna kan även kommentarer i fritextfält lämnas. Inför utvecklingssamtalen bedömer och dokumenterar lärarna elevernas utveckling på ett antal områden, t.ex. kommunikation, samarbete och kreativitet. Dessa bedömningar dokumenteras i fritextfält.

Det finns inga rutiner och riktlinjer för hur dokumentationen kring IUP med skriftliga omdömen ska göras. Det finns inga skriftliga rutiner och riktlinjer för vilken information som är relevant att lämna i de fritextfält som finns i Skolportalen.

Åtkomst till uppgifter i Skolportalen sker via Internet för elever, vårdnadshavare, lärare, skolledning och mentor. Samtliga dessa användare har olika roller och behörigheter i Skolportalen.

En vårdnadshavare kan ta del av uppgifter om andra elever (klasslista med kontaktuppgifter), personallista och schema. För sitt barn får vårdnadshavaren del av samtalsunderlag inför utvecklingssamtal, sammanställning av utvecklingssamtal, grupplistor med kontaktuppgifter, mentorslistor, betyg/omdömen och frånvaro.

Lärare/mentorerna kan ta del av personalens scheman, personallistor, uppgift om skolans elever (namn, adress, telefonnummer, födelsedatum, e-post, klass), samtliga elevers scheman, sammanställningar av samtliga elevers frånvaro, klass- och grupplistor, betyg/omdömen för sina egna elever och mentorselever, samtalsunderlag och utvecklingsmål för sina elever.

Åtkomst till uppgifter i Skolportalen sker genom inloggning med användarnamn och lösenord (komplexitetskrav finns). Till vårdnadshavarna skickas lösenordet brevlades till folkbokföringsadressen. Det lösenordet är en aktiveringskod som vårdnadshavarna uppmanas att byta vid första inloggningen. Behörigheten för vårdnadshavare tas automatiskt bort när eleven fyller 18 år eller vid förlust av vårdnad.

Elever och personal får sina användaruppgifter av skolans Extens-administratör och även för eleverna är det första lösenordet en aktiveringskod.

Nämnden avser under år 2010 använda en ny metod för åtkomst till uppgifter i Skolportalen via Internet, bestående av användarnamn, lösenord samt engångslösenord. Detta sätt att logga in i systemet kommer inte att omfatta elever, utan det riktar sig till skolpersonal och vårdnadshavare.

Det är oklart om samtliga vårdnadshavare/elever informeras om personuppgiftsbehandlingen i Extens/Skolportalen. På kommunens hemsida finns viss information tillgänglig genom dokumentet "Information och samtycke till registrering i Skolportalen". Någon riktad informationsinsats sker inte.

På kommunens hemsida, där vårdnadshavare ges möjlighet att logga in i Skolportalen, finns följande information.  
"För att få tillgång till många av Skolportalens funktioner måste ni logga in. GENOM ATT LOGGA IN, samtycker ni till hantering utav personuppgifter i Tyresö kommuns Skolportal. Information om denna hantering, finner ni till vänster i dokumentet under::Länkar."

I informationen under "Länkar" anges exempelvis att registreringen i Skolportalen är frivillig. Någon kontroll av att vårdnadshavare verkligen tagit del av informationen om personuppgiftsbehandlingen innan inloggning sker inte. De vårdnadshavare som inte besöker Tyresö kommuns hemsida och där loggar in på Skolportalen får ingen information om hanteringen av personuppgifter i Skolportalen. Inte heller inhämtas deras samtycke.

Vårdnadshavare har möjlighet att motsätta sig att dokumentationen kring IUP med skriftliga omdömen görs i Skolportalen. Någon information till

samtliga vårdnadshavare om denna möjlighet ges inte. Enligt uppgift arbetar nämnden med frågan.

Det sker ingen gallring av personuppgifter i Extens/Skolportalen. Rutiner för gallring är under konstruktion.

För viss support av Extens/Skolportalen anlitas ett externt företag. Nämnden har ett personuppgiftsbiträdesavtal med företaget.

## **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. Instruktionerna bör exempelvis ange hur värderande omdömen om eleven skall formuleras och att kränkande uttalanden inte är tillåtna. Sådana instruktioner kan för skolors vidkommande exempelvis ta sin utgångspunkt i relevanta dokument från Skolverket. För dokumentation av IUP med skriftliga omdömen kan exempelvis nämnas Skolverkets allmänna råd om den individuella utvecklingsplanen med skriftliga omdömen.

I ärendet har framkommit att det förekommer flera fritextfält i Skolportalen. Dessa fritextfält finns för den dokumentation som sker i samband med utvecklingssamtal och IUP med skriftliga omdömen. Nämnden har inga skriftliga rutiner för vad som får antecknas i fritextfälten och hur användarna bör uttrycka sig. Inte heller är det möjligt för användarna att välja fasta, i förväg angivna, alternativa formuleringar. Det är Datainspektionens bedömning att det, särskilt mot bakgrund av att användarna i fritextfälten dokumenterar elevernas färdigheter och sociala utveckling i övrigt, behövs skriftliga instruktioner och riktlinjer för den dokumentation som sker i fritextfälten.

Datainspektionen förutsätter att nämnden, om den vill fortsätta att behandla personuppgifter i fritextfälten i Extens/Skolportalen, utfärdar skriftliga

instruktioner till användarna om vilka uppgifter som är relevanta att lämna i fritextfältet. Datainspektionen vill att nämnden senast den 30 april 2010 lämnar in en redogörelse till Datainspektionen för vilka skriftliga instruktioner som har utfärdats.

#### *Känsliga personuppgifter*

I 13 § PuL finns ett grundläggande förbud mot att behandla känsliga personuppgifter som t.ex. avslöjar ras, etniskt ursprung, politiska åsikter eller rör hälsa och sexualliv. 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.

I ärendet har framkommit att uppgift om sjukdom kan behandlas genom de förvalda orsaksalternativen i frånvarorapporteringen, utan att nämnden inhämtar uttryckligt samtycke till behandling av känsliga personuppgifter (för övriga frågor rörande samtycke se under rubriken ”samtycke till personuppgiftsbehandling”).

Datainspektionen vill i sammanhanget framhålla att en uppgift om att en elev är sjuk eller t.ex. på läkarbesök är, alldeles oavsett om symptom eller diagnos anges, en känslig personuppgift i personuppgiftslagens mening.

Datainspektionen förutsätter att nämnden, om den vill fortsätta behandla känsliga personuppgifter i Extens/Skolportalen, inhämtar uttryckligt samtycke till sådan behandling. Datainspektionen vill att nämnden senast den 30 april 2010 lämnar in en redogörelse till Datainspektionen för hur ett eventuellt samtycke har inhämtats.

#### *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.”

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.

I ärendet har framkommit att nämnden behandlar känsliga personuppgifter (uppgift om sjukdom) i frånvarorapporteringen. Det har även framkommit att nämnden behandlar integritetskänsliga uppgifter, vilket utgörs av de uppgifter som dokumenteras inför utvecklingssamtal och vid framtagandet av IUP med skriftliga omdömen. Värderande omdömen om elevers sociala utveckling, exempelvis elevers förmåga att kommunicera, samarbeta och vara kreativa är enligt Datainspektionen, typiskt sett, integritetskänsliga uppgifter nära kopplade till elevernas personliga förhållanden och privata sfär.

Vidare har framkommit att användarna har åtkomst till Skolportalen över Internet genom inloggning med användarnamn och lösenord.

Behandlingen av personuppgifter i Skolportalen uppfyller därmed inte säkerhetskraven i PuL beträffande känsliga och integritetskänsliga personuppgifter. Datainspektionen finner det anmärkningsvärt att nämnden inte åtgärdat denna brist tidigare, inte minst mot bakgrund av Datainspektionens tillsynsbeslut mot nämnden i september 2008. I sammanhanget skall hänsyn emellertid tas till att nämnden har för avsikt att under 2010 introducera en ny metod för åtkomst till uppgifter i Skolportalen, bestående av användarnamn, lösenord samt engångslösenord.

Mot bakgrund av ovanstående förutsätter Datainspektionen att nämnden förverkligar sin avsikt att under 2010 vidta tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifter i Skolportalen. Datainspektionen vill att nämnden senast 30 april 2010 lämnar in en redogörelse till Datainspektionen för hur dessa åtgärder har omhändertagits.

#### *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 nämnden inte gallrar uppgifter i Extens/Skolportalen, eller har några riktlinjer och rutiner för bevarande. Vidare framgår, enligt nämnden, att rutiner för gallring är under konstruktion.

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 nämnden 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 nämnden 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 nämnden i sitt fortsatta arbete, på uppgiftsnivå, analyserar och utvärderar behovet av bevarande av uppgifter i Extens/Skolportalen och utifrån detta tar fram riktlinjer och rutiner för bevarande och gallring av personuppgifter. Datainspektionen vill att nämnden 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.

### *Information till registrerade*

I PuL finns ett flertal bestämmelser om information om och samtycke till behandling av personuppgifter. I lagens 23 § anges följande.

”Om uppgifter om en person samlas in från personen själv, skall den personuppgiftsansvarige i samband därmed självmant lämna den registrerade information om behandlingen av uppgifterna.”

Vidare anges i 25 § första stycket PuL följande.

”Information enligt 23 eller 24 § skall omfatta

- a) uppgift om den personuppgiftsansvariges identitet,
- b) uppgift om ändamålen med behandlingen, och
- c) all övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse.

Bestämmelsen innebär att den personuppgiftsansvarige måste informera elever eller vårdnadshavare om hur deras personuppgifter behandlas i IT-systemen. Den personuppgiftsansvarige måste informera om vem som ansvarar för systemen (vem som är personuppgiftsansvarig), vilka personuppgifter som samlas in, vad uppgifterna ska användas till samt att den registrerade har rätt att ansöka om information (få ett s.k. registerutdrag) och begära rättelse av felaktiga uppgifter. Informationen bör lämnas till eleverna själva om de kan tillgodogöra sig informationen. Om så inte är fallet, till exempel då det är fråga om yngre barn, skall informationen i stället lämnas till vårdnadshavaren. Informationen måste inte lämnas skriftligen utan kan istället lämnas muntligen. Det kan dock vara lämpligt att informera genom ett informationsblad som delas ut till samtliga vårdnadshavare och elever, exempelvis vid läsårets början.

I ärendet har framkommit att det inte sker någon riktad informationsinsats rörande personuppgiftsbehandlingen i Extens/Skolportalen och att nämnden inte vet om samtliga elever/vårdnadshavare informeras om personuppgiftsbehandlingen. På kommunens hemsida finns dock viss information tillgänglig.

Enligt Datainspektionen är det inte tillräckligt att information finns tillgänglig på kommunens hemsida. Detta eftersom det inte kan antas att samtliga elever/vårdnadshavare har möjlighet att tillgodogöra sig informationen om den endast finns åtkomlig på Internet.

Mot bakgrund av ovanstående förutsätter Datainspektionen att nämnden vidtar åtgärder för att se till att elever och vårdnadshavare får fullständig information om den personuppgiftsbehandling som sker i Extens/Skolportalen. Datainspektionen vill att nämnden senast den 30 april 2010 lämnar in en redogörelse till Datainspektionen för hur arbetet med vidta åtgärder för att fullgöra informationsplikten har omhändertagits.

#### *Samtycke till personuppgiftsbehandling*

En grundregel i PuL är att personuppgifter får behandlas endast efter samtycke från den registrerade. Från denna huvudregel finns emellertid ett flertal undantag. För den personuppgiftsbehandling som sker för elevadministrativa ändamål torde det sällan ställas krav på inhämtande av de registrerades samtycke. Detta åtminstone så länge nämnden inte behandlar känsliga personuppgifter för elevadministrativa ändamål, vill publicera uppgifter öppet på Internet eller behandla redan insamlade uppgifter för något nytt ändamål som är oförenligt med det ursprungliga ändamålet.

I ärendet har framkommit att det på kommunens hemsida finns följande information.

”För att få tillgång till många av Skolportalens funktioner måste ni logga in. GENOM ATT LOGGA IN, samtycker ni till hantering utav personuppgifter i Tyresö kommuns Skolportal. Information om denna hantering, finner ni till vänster i dokumentet under::Länkar.”

I informationen under ”Länkar” framgår bl.a. att registreringen i Skolportalen är frivillig.

Vidare har i ärendet framgått att vårdnadshavare har möjlighet att motsätta sig att dokumentationen kring IUP med skriftliga omdömen görs i Skolportalen. Någon information till samtliga vårdnadshavare om denna möjlighet ges emellertid inte.

Datainspektionen anser att det är oklart vad nämnden, med ovanstående formuleringar, avser att inhämta samtycke till. I sammanhanget vill Datainspektionen särskilt poängtera vikten av att den personuppgiftsansvarige, innan ett samtycke inhämtas, lämnar korrekt information så att den registrerade vet vad samtycket innebär och omfattar.

Upplysningsvis vill Datainspektionen även framhålla att den personuppgiftsansvarige inte har någon skyldighet att inhämta samtycke till behandling av personuppgifter om det inte följer av personuppgiftslagen eller annan författning. I själva verket kan det till och med vara olämpligt att

inhämta samtycke till en personuppgiftsbehandling som den personuppgiftsansvarige har laglig grund för eller till och med rättsliga krav på att utföra utan att samtycke inhämtas.

Datainspektionen förutsätter att nämnden gör en analys av ovan nämnda samtyckeshantering och, om nämnden bedömer att samtycke verkligen behöver inhämtas, lämnar relevant information som gör det tydligt för den registrerade vad samtycket omfattar. Om nämnden även fortsättningsvis avser att ge vårdnadshavare möjlighet att motsätta sig att vissa personuppgifter, men inte andra, behandlas i Skolportalen förutsätter Datainspektionen att nämnden tydliggör hur ett sådant motsättande förhåller sig till ett eventuellt samtycke. Datainspektionen vill att nämnden senast den 30 april 2010 lämnar in en redogörelse till Datainspektionen för hur denna analys har gjorts och vad den har resulterat i.

### **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-säkerhetsspecialisten Magnus Bergström och juristerna Ulrika Harnesk och Patrik Sundström, föredragande.

Erik Janzon

Patrik Sundström