



**Beslut**  
2008-09-09

**Dnr**  
128-2008

Internationella Engelska Skolan AB  
Styrelsen  
Nytorpsvägen 5A  
183 53 Täby

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

### **Datainspektionens beslut**

Datainspektionen konstaterar att Internationella Engelska Skolan AB (härefter bolaget) har behandlat personuppgifter i strid med personuppgiftslagen.

Datainspektionen förutsätter att bolaget beaktar de påpekanden som framförs i detta beslut (under rubriken Datainspektionens bedömning) rörande:

- Personuppgifter i fritextfält
- Känsliga personuppgifter
- Säkerhetsåtgärder
- Personuppgiftsbiträdesavtal
- Bevarande och gallring
- Information till de registrerade
- Behörigheter och åtkomst till patientuppgifter i skolhälsovården
- Kontroll av åtkomst till patientuppgifter i skolhälsovården

Ärendet avslutas men kan komma att följas upp.

### **Bakgrund**

Med anledning av uppgifter i dagspressen om brister i bolagets personuppgiftsbehandling inledde Datainspektionen tillsyn mot bolaget och genomförde inom ramen för tillsynen inspektioner i bolagets skolor i Gävle och Täby den 18 respektive 20 februari 2008.

Under tillsynen har bl.a. följande framkommit.

Skolornas elevadministrativa system var vid inspektionstillfällena EasySchool. Detta system användes i allt väsentligt på samma sätt vid bolagets skolor i Gävle och Täby.

Bolaget har upplyst att man efter inspektionerna har ersatt EasySchool med SchoolSoft i samtliga skolor som hör till bolaget.

### EasySchool

I EasySchool registreras frånvaro, ämnesprestationer och uppförande. De som har åtkomst till uppgifterna är elever, lärare och vårdnadshavare. Systemet är webbaserat och körs genom en webbläsare.

När man i frånvaroregistreringen, under fliken ”Absence”, anger frånvaroorsak kan man välja både ett fast alternativ i en rullningslist och skriva i ett fritextfält. I detta fritextfält kan även sådant skrivas in som inte rör elevens frånvaro, t.ex. hur eleven har uppfört sig eller hur eleven har presterat i ett visst ämne. I frånvaroregistreringen kan man, förutom att skriva i fritextfältet, välja olika fasta koder från en rullningslist. S betyder sjuk, H betyder skollov, D betyder besök hos läkare (ej hos skolhälsovården). I fritextfältet görs även noteringar som rör elevens uppförande.

Det finns fritextfält i flera delar av systemet. Det saknas skriftlig policy för vad som får skrivas in i fritextfälten, men lärarna informeras om vad som ska skrivas in och viss vägledning ges i personalhandboken.

Användare loggar in i systemet över Internet med hjälp av användarnamn och lösenord. Lösenord och användarnamn delas ut på kvällsmöten som hålls med vårdnadshavarna. Vid dessa möten bockar man av användarna som skriver under att de fått lösenord och användarnamn. När lösenord och användarnamn delas ut behöver vårdnadshavarna inte legitimera sig, det räcker att de uppger att de är vårdnadshavare till visst barn. Då får de en papperslapp på vilken lösenord och användarnamn står antecknade. Om en användare glömmet användarnamn och lösenord, skickas dessa ut till användaren via e-post.

Det lämnas ingen information om rättigheter enligt personuppgiftslagen vid kvällsmötena och inte heller vid något annat tillfälle. Bolaget har uppgivit att de vårdnadshavare som ansöker om plats i skolan via bolagets hemsida, informeras om att uppgifterna kommer att sparas digitalt och bearbetas av skolans personal.

Inget samtycke till behandling av personuppgifter inhämtas, varken skriftligt eller muntligt.

Driften av EasySchool sköts för hela bolaget av företagen Easy Interaction och 24 Solutions. 24 Solutions driftar även bolagets nät och servrar.

Bolaget har inga personuppgiftsbiträdesavtal med Easy Interaction och 24 Solutions.

Det sker ingen gallring av gamla elevers personuppgifter.

### Profdoc

Profdoc är det journalföringssystem som skolhälsovården använder sig av vid bolagets skolor. Bara skolsköterskan och skolläkaren har åtkomst till uppgifterna i Profdoc.

Skolsköterskan har även åtkomst till journaler för elever som lämnat skolan. När en elev byter skola, ges den nya skolan åtkomst till elevens journal. Detta sköts av leverantören som är Profdoc och som driftar systemet.

Bolaget vet inte hur loggarna hanteras i Profdoc. Det görs inga kontroller av vem som haft tillgång till viss journal. Det skapas inte automatiskt en notering i den elektroniska journalen när någon öppnar journalen i fråga.

I Profdoc kan Täbyskolans skolsköterska även komma in i journaler för elever som går i någon annan av bolagets skolor.

#### Micromarc

I Täbyskolan finns det ett bibliotekssystem – Micromarc – som innehåller elevernas personuppgifter. De uppgifter som behandlas i systemet är elevens namn, personnummer, hemadress och klass samt vårdnadshavarnas namn och adress och vilka böcker eleven har lånat. Alla elever läggs in i Micromarc, även om de inte lånar någon bok.

Micromarc driftas av Bibliotekscentrum. Bolaget vet inte hur länge elevernas personuppgifter bevaras i Micromarc.

#### **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 framkommit att bolaget vid inspektionstillfällena saknade skriftliga instruktioner för vad som får skrivas in i fritextfälten, men att lärarna ges viss vägledning i personalhandboken.

Om bolaget även fortsättningsvis vill använda sig av fritextfält, förutsätter Datainspektionen att bolaget utfärdar skriftliga instruktioner till användarna som på ett tydligt sätt anger 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.

I ärendet har framkommit att uppgifter om sjukdom vid inspektionstillfällena behandlades i EasySchool, både i fritextfält och i fasta koder i en rullningslist. Vidare har framkommit att bolaget inte inhämtade uttryckligt samtycke till behandlingen av känsliga personuppgifter.

Om bolaget även fortsättningsvis vill behandla känsliga personuppgifter i sitt skoladministrativa system, förutsätter Datainspektionen att bolaget 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 följande framkommit. Vid inspektionstillfällena behandlade bolaget i EasySchool både känsliga och andra integritetskänsliga uppgifter; dessa var uppgifter om sjukdom, frånvaro, besök hos läkare och uppgifter om elevernas uppförande. Användarna hade åtkomst till EasySchool över Internet och Internetinloggning i EasySchool skedde med endast användarnamn och lösenord. Vårdnadshavarna behövde inte legitimera sig när lösenord och användarnamn delades ut, det räckte att de uppgav att de är vårdnadshavare till ett visst barn. Användarnamn och lösenord skickades via e-post till användare som glömt dem.

Därmed behandlade bolaget känsliga och andra integritetskänsliga personuppgifter i EasySchool utan att uppfylla säkerhetskraven i 31 § PuL beträffande känsliga och andra integritetskänsliga personuppgifter.

Om bolaget även fortsättningsvis vill behandla känsliga och andra integritetskänsliga personuppgifter i sitt skoladministrativa system och göra dessa uppgifter åtkomliga över Internet, förutsätter Datainspektionen att bolaget

- vidtar tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifterna i systemet (dvs. börjar använda sig av asymmetrisk kryptering, exempelvis e-legitimation, engångslösenord eller motsvarande)
- försäkras sig om att endast vårdnadshavare får del av inloggningsuppgifter (exempelvis genom att inloggningsuppgifter ges endast till dem vars identitet bolaget har personlig kännedom om, eller skickas med post till vårdnadshavarnas folkbokföringsadresser)
- endast skickar lösenord till vårdnadshavare med e-post om meddelandet krypteras på ett sådant sätt att bara den avsedda mottagaren kan del av meddelandets innehåll.

- 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 driften av flera av bolagets system vid inspektionstillfällena sköttes av utomstående företag och att det i flera fall saknades personuppgiftsbiträdesavtal med dessa företag.

Datainspektionen förutsätter att bolaget ingår sådana avtal med alla 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.*

I ärendet har framkommit att bolaget vid inspektionstillfällena saknade riktlinjer och rutiner för bevarande och gallring av personuppgifter i sina system.

Datainspektionen förutsätter därför att bolaget tar fram riktlinjer och rutiner för bevarande och gallring av personuppgifter, vilka även omfattar de behandlingar som personuppgiftsbiträdena utför för bolagets räkning.

- Information till de registrerade

I PuL finns bestämmelser om information som ska lämnas till den registrerade. I lagens 23 § anges följande.

*Om uppgifter om en person samlas in från personen själv, skall den personuppgiftsansvarige i samband därmed självständigt 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.*

Bestämmelserna 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, ska 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.

Bolaget har uppgivit att de vårdnadshavare som ansöker om plats i skolan via bolagets hemsida, informeras om att uppgifterna kommer att sparas digitalt och bearbetas av skolans personal.

I övrigt lämnade bolaget vid inspektionstillfällena ingen information om den personuppgiftsbehandling som bolaget utför. Det innebär att bolaget varken informerade om den omfattande personuppgiftsbehandling som sker avseende eleverna när de går i någon av bolagets skolor, eller om rätten till registerutdrag och rättelse.

Datainspektionen förutsätter att bolaget fortsättningsvis ger vårdnadshavarna och eleverna fullständig information om den personuppgiftsbehandling som sker vid bolagets skolor.

- Behörigheter och åtkomst till patientuppgifter i skolhälsovården

För behandling av personuppgifter inom skolhälsovården gäller, förutom PuL, bestämmelserna i patientdatalagen (2008:355) och Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14).

I 4 kap. 1 § patientdatalagen anges följande beträffande inre sekretess.  
*Den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.*

I 4 kap. 2 § första stycket patientdatalagen anges följande med avseende på tilldelning av behörighet.  
*En vårdgivare ska bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.*

I 2 kap. 6 § första och andra stycket i Socialstyrelsens nämnda föreskrift anges följande.  
*Vårdgivaren ska ansvara för att det i ledningssystemet finns rutiner som säkerställer att hälso- och sjukvårdspersonalens och andra befattningshavares behörighet begränsas till vad som är nödvändigt för att ge en god och säker vård.*

*Vårdgivaren ska vidare ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till patientuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys.*

I ärendet har framkommit att det var möjligt för en skolsköterska att i Profdoc även komma in i journaler för elever som gick i någon annan av bolagets skolor. Av ovan återgivna bestämmelser framgår emellertid att en sådan vidsträckt behörighet endast får förekomma om det är nödvändigt för att ge en god och säker vård.

Datainspektionen förutsätter därför att bolaget tar fram rutiner som säkerställer att användarnas behörigheter i Profdoc begränsas till vad som är nödvändigt för att ge en god och säker vård.

- Kontroll av åtkomst till patientuppgifter i skolhälsovården

I 4 kap. 3 § första stycket patientdatalagen anges följande.

*En vårdgivare ska se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras. Vårdgivare ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter.*

I 2 kap. 11 § Socialstyrelsens ovan nämnda föreskrift anges följande rörande åtkomstkontroll.

*Vårdgivaren ska ansvara för att det i ledningssystemet finns rutiner som säkerställer att*

- 1. det av dokumentationen av åtkomsten (loggarna) framgår vilka åtgärder som har vidtagits med patientuppgifterna*
- 2. det av loggarna framgår vid vilken vårdenhet och vid vilken tidpunkt åtgärderna har vidtagits,*
- 3. användarens och patientens identitet framgår av loggarna,*
- 4. systematiska och återkommande stickprovskontroller av loggarna görs,*
- 5. genomförda kontroller av loggarna dokumenteras, och*
- 6. loggarna sparas i minst tio år.*

I ärendet har framkommit att bolaget vid inspektionstillfällena saknade rutiner som säkerställer att logguppföljningar faktiskt utförs. Datainspektionen förutsätter därför att bolaget tar fram sådana rutiner.

### **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 Ni fick ta del av beslutet 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