

Utbildningsnämnden  
Knivsta kommun  
741 75 KNIVSTA

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

### **Datainspektionens beslut**

Datainspektionen konstaterar att Utbildningsnämnden i Knivsta kommun (härefter nämnden):

1. behandlar personuppgifter i fritextfälten i Extens och Unikum i strid med kravet i 9 § PuL på särskilda, uttryckligt angivna och berättigade ändamål
2. behandlar känsliga personuppgifter i Extens 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 samt behörighetsstyrningen i Unikum)
4. behandlar personuppgifter i Extens och Unikum 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 utan att informera de registrerade om behandlingen
6. inhämtar samtycke vid användning av Unikum 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 och Unikum.
2. Inhämtar samtycke till behandlingen av känsliga personuppgifter i Extens.
3. Vidtar åtgärder dels för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifter i Unikum, dels för att se över hur rutinerna för behörighetsstyrning fungerar i praktiken.
4. Tar fram riktlinjer och rutiner för bevarande och gallring av personuppgifter i Extens och Unikum.

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

Senast den 30 april 2010 skall nämnden inkomma med en redogörelse till Datainspektionen för hur arbetet med att ta fram rutiner och riktlinjer för bevarande och gallring av personuppgifter i Extens och Unikum har omhändertagits.

Ärendet avslutas men kan komma att följas upp.

### **Bakgrund**

Datainspektionen genomförde den 6 oktober 2009 en inspektion av nämndens personuppgiftsbehandling på Thunmanskolan.

Under inspektionen, har bl.a. följande framkommit.

De IT-stöd som används på Thunmanskolan som innehåller personuppgifter om elever, och i förekommande fall vårdnadshavare, är bl.a. Extens och Unikum. Det finns ett skolnät och ett administrativt nät.

### ***Extens***

Extens är ett system för elevregistrering, schemaläggning och frånvarohantering. Inloggning sker separat till systemet med användarnamn och lösenord. Var tredje månad sker ett tvingande lösenordsbyte.

De personuppgifter om elever som behandlas i Extens är namn, personnummer, adress, klass, utbildningsform (program), lärare, schema, frånvaro, betyg, resultat från nationella prov samt modermål. För de elever som deltar i barnomsorgen och fritidsverksamhet finns även vårdnadshavares personuppgifter och inkomstuppgifter samt eventuellt syskon.

Endast administrativ och pedagogisk personal har tillgång till Extens. Det finns ingen möjlighet till webbåtkomst. Pedagogisk personal kan se alla elever på skolan samt registrera frånvaro för dessa. Betyg kan endast sättas för egna elever.

Skolan beställer skriftligen behörighet för eleverna till systemet från kommunens IT-avdelning som lägger upp konton. När personal slutar ska skolan avbeställa behörigheten via en blankett. Har ett konto inte använts på 3 månader sker en manuell låsning av kontot. Nytt lösenord krävs för att

reaktivera kontot. Det sker en årlig manuell avstämning av samtliga behörigheter till Extens.

Registrering av frånvaro sker genom förvalda alternativ, bl.a. orsaken "sjuk" och "läkare". Möjlighet till kortfattade fria anteckningar finns men inga skriftliga rutiner för hur de ska användas. Dock diskuteras detta vid användarmöten.

Någon information om behandlingen i Extens har inte getts till elever eller vårdnadshavare och inget samtycke har hämtats in.

Ingen gallring av personuppgifter i Extens har skett sedan 2003.

Personuppgiftsbiträdesavtal finns med bolaget IST som kan tillåtas åtkomst till systemet på distans för service och support. IST har satt igång ett projekt kring gallring av uppgifter i Extens.

### ***Unikum***

Unikum är ett system för hantering av individuella utvecklingsplaner (IUP) samt skriftliga omdömen. Den rättsliga grunden för behandlingen av elevernas personuppgifter i systemet uppges vara kommunens myndighetsutövning. Inget samtycke har hämtats in.

Personuppgifter om elever som behandlas i Unikum är namn, personnummer, klass samt eventuell e-postadress. Om vårdnadshavare begär tillgång till systemet behandlas även deras namn, personnummer, adress, e-postadress och koppling till barnen. Vårdnadshavare får lämna samtycke till behandlingen av deras egna personuppgifter. De uppgifter som behandlas för personal är namn och personnummer. Grunduppgifter avseende elever hämtas från Extens.

Unikum används av personal, elever och i förekommande fall vårdnadshavare.

Behörighet för elever och vårdnadshavare läggs upp av elevens mentor som registrerar personuppgifterna samt lägger upp konton. Personalens behörighet läggs upp av IT-piloten. Lärare kan se historik för sina elever.

Inför varje termin läggs en ny IUP-katalog upp. Efter terminens slut läses katalogen. Vid starten av en ny termin ska mentorn, för sin mentorsgrupp, koppla behörighet till elevuppgifter endast till aktuella undervisande lärare. Vid förevisning av Unikum framkommer att en person har tillgång till uppgifter om elever denne tidigare varit mentor för. Personen var inte upplagd som lärare för en av de klasser som personen undervisade.

Inloggning sker med användarnamn och lösenord. Vid första inloggningen sker ett tvingande byte av lösenord. Inloggningsuppgifter skickas via e-post eller lämnas ut av mentorn. Om man har glömt lösenordet skickas ett nytt tillfälligt lösenord ut via e-post. Därefter sker ett tvingande lösenordsbyte.

En lathund för lärarnas användning av Unikum finns. Information till vårdnadshavare om Unikum gick ut vid införandet av systemet. Dokument rörande hantering av personuppgifter i webbverktyget för IUP med skriftliga omdömen har getts in.

Vid förevisningen av Unikum framkommer att under rubriken "Skriftliga omdömen" har exempelvis följande kommentar lämnats av en lärare: "Jag blir arg och upprörd när eleverna inte har ordning på sina saker. Och när det transas och pratas ideligen samt när elever kommer för sent. Inte så konstigt????"

Vid överföring av uppgifter från Unikum till friskola eller skola i annan kommun inhämtas samtycke från vårdnadshavare.

Ingen gallring av uppgifter i Unikum sker för närvarande. Vad som händer med skolans uppgifter om elever som slutar på Thunmanskolan är oklart.

Åtkomst till Unikum sker endast via webben. Systemet driftas av Unikum. Personuppgiftsbiträdesavtal finns.

## **Datainspektionens bedömning**

### ***Extens***

#### *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 och i fritextfälten i frånvarorapporteringen, utan att nämnden inhämtar uttryckligt samtycke till behandling av känsliga personuppgifter.

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, inhämtar uttryckligt samtycke till sådan behandling.

#### *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 att kränkande uttalanden inte är tillåtna.

I ärendet har framkommit att Extens innehåller möjlighet till kortfattade anteckningar i fritextfält i samband med frånvaroregistrering. Vidare har framkommit att nämnden inte har några skriftliga rutiner och instruktioner för dokumentationen i fritextfält.

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

#### *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 ingen information getts till elever och vårdnadshavare rörande personuppgiftsbehandlingen i Extens.

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.

## **Unikum**

### *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 integritetskänsliga personuppgifter, vilket utgörs av de uppgifter som dokumenteras vid framtagandet av IUP med skriftliga omdömen. Värderande omdömen om 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 Unikum över Internet genom inloggning med användarnamn och lösenord.

Behandlingen av personuppgifter i Unikum uppfyller därmed inte säkerhetskraven i PuL beträffande integritetskänsliga personuppgifter. Datainspektionen förutsätter att nämnden vidtar tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifter i Unikum.

#### *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 Unikum. Exempelvis har under rubriken "Skriftliga omdömen" kommentaren "Jag blir arg och upprörd när eleverna inte har ordning på sina saker. Och när det tramsas och pratas ideligen samt när elever kommer för sent. Inte så konstigt????" lämnats av en lärare. Vid inspektionen på Thunmanskolans uppgav nämnden att det finns en lathund för lärarnas användning av Unikum. I den dokumentation nämnden gav in i ärendet anges dock endast att i Unikum ska inga känsliga uppgifter lagras då IUP och skriftliga omdömen är allmänna handlingar. Inte heller uppgifter om frånvaro ska hanteras i Unikum. Mot bakgrund av att användarna i fritextfälten dokumenterar elevernas färdigheter och utveckling är dessa instruktioner, enligt Datainspektionens bedömning, inte tillräckliga.

Datainspektionen vill i sammanhanget framhålla att den bedömning som görs enligt offentlighets- och sekretesslagen (2009:400) skiljer sig från bedömningen av om själva behandlingen av personuppgifter är tillåten enligt PuL.

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

#### *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 vid den första inloggningen till Unikum krävs samtycke till villkoren för användning av verktyget. I användarvillkoren som då visas anges att användaren måste ge sitt samtycke till "hur information lagras, används och visas i Unikums tjänst". Vidare anges att "i Unikum lägger föräldrar, barn, elever, lärare och skolpersonal in personuppgifter och annat material som används i förskola, under skolgång och vid annat lärande". Under rubriken "Ytterligare information" anges dock att samtycket till att använda Unikum endast handlar om användarens egen användning av

verktyget. Oavsett om samtycke finns kan skolan välja att använda Unikum för att hantera uppgifter om elever och vårdnadshavare.

Datainspektionen anser att det för användaren, med denna utformning av informationen, inte är tydligt vad samtycket egentligen omfattar.

Datainspektionen förutsätter att nämnden gör en analys av ovan nämnda samtyckeshantering och lämnar relevant information som gör det tydligt för den registrerade vad samtycket omfattar.

#### *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 skriftliga rutiner för tilldelning av behörighet till Unikum finns. Av denna kan utläsas att en mentor/lärare endast ska ha åtkomst till elevdokumentation, IUP och omdömen för elever som denne arbetar med eller har som mentorselever. Vid inspektionen framkom emellertid att en person fortfarande hade åtkomst till uppgifter om elever denne tidigare varit mentor för. Personen hade däremot inte åtkomst till elever i en klass där personen för tillfället undervisade.

Mot bakgrund av ovanstående förutsätter Datainspektionen att nämnden ser över hur rutinerna för behörighetsstyrningen till Unikum fungerar i praktiken.

#### *Extens/Unikum*

##### *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 och Unikum.

Att personuppgifter som inte längre behövs skall gallras är en av hörnstenarna i integritetsskyddslagstiftningen. Att samtliga personuppgifter 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 har 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 rättsskipning 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, på uppgiftsnivå, analyserar och utvärderar behovet av bevarande av uppgifter i Extens och Unikum 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.

I sammanhanget vill Datainspektionen upplysningsvis informera om vikten av att nämnden även försäkras om att personuppgiftsbiträdet 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-säkerhetsspecialisten Magnus Bergström och juristerna Patrik Sundström och Ulrika Harnesk, föredragande.

Erik Janzon

Ulrika Harnesk