

Produktionsnämnden för vård och bildning
Uppsala kommun
753 75 UPPSALA

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

Datainspektionens beslut

Datainspektionen konstaterar att Produktionsnämnden för vård och bildning i Uppsala 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 Skola24 i strid med kravet i 15 § PuL på samtycke
3. behandlar känsliga personuppgifter i strid med kravet i 31 § PuL på att vidta tillräckliga säkerhetsåtgärder
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 ändamålet med behandlingen
6. behandlar personuppgifter i Skola24, utan att informera de registrerade om 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 Skola24
3. vidtar tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifterna i Skola24 och endast skickar lösenord till vårdnadshavare med e-post om meddelandet krypteras på ett sådant sätt att bara den avsedda mottagaren kan ta del av meddelandets innehåll
4. ingår personuppgiftsbiträdesavtal med sina personuppgiftsbiträden
5. tar fram riktlinjer och rutiner för gallring av personuppgifter i Skola24, Rexnet och Extens
6. ger vårdnadshavarna och eleverna fullständig information om den personuppgiftsbehandling som sker i Skola24.

Ärendet avslutas, men kan komma att följas upp

Redogörelse för tillsynsärendet

Datainspektionen genomförde den 9 maj 2008 en inspektion av nämndens personuppgiftsbehandling i Vaksalaskolan.

Vid inspektionen framkom bl.a. följande.

För registrering av frånvaro för elever i årskurs 7-9 används systemet Skola24. Frånvaroorsaken kan anges med hjälp av fasta menyval. Som frånvaroorsak kan anges bl.a. ”sjukanmäld” och ”läkar- och tandläkarbesök”.

I Skola24 finns ett fritextfält som är valbart för varje skola. I Vaksalaskolan används fritextfältet och man har en lokal rutin för hur fritextfältet skall användas. Elever och/eller vårdnadshavare får ingen information om, och samtycker heller inte till, den personuppgiftsbehandling som sker i Skola24.

Lärare och vårdnadshavare har åtkomst till Skola24. Inloggning sker med användarnamn och lösenord. Vårdnadshavarna får inloggningsuppgifterna via e-post.

Efter inspektionen har framkommit att frånvarooanledningen ”läkar- och tandläkarbesök” inte kan ses av vårdnadshavarna. Vidare pågår en översyn där nämnden räknar med att reducera antalet frånvarooanledningar för att säkerställa att de är lagliga.

Tekniskt underhåll och drift av Skola24 sköts av Novasoftware. Nämnden saknar personuppgiftsbiträdesavtal med Novasoftware.

På skolan används utbildningsplattformen Rexnet, till vilken elever och lärare har åtkomst via Internet. I en annan kommunal skola i Uppsala har vårdnadshavare släppts in i Rexnet på prov. Inloggning sker med hjälp av användarnamn och lösenord. All kommunikation skyddas med https.

Tekniskt underhåll och drift av Rexnet sköts av Tietoenator. Nämnden saknar personuppgiftsbiträdesavtal med Tietoenator.

Nämnden använder systemet Extens för att registrera uppgifter som elevens betyg, språkval, modersmål och resultat från nationella prov.

Nämnden har ingen kännedom om och i så fall när personuppgifter gallras i de olika systemen.

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 användandet av fritextfältet i Skola24 är frivilligt för varje skola. På Vaksalaskolan finns en lokal rutin för hur fritextfältet skall användas. Nämnden har dock inte, enligt vad som framkommit i ärendet, utfärdat några centrala skriftliga rutiner för vad som får skrivas in i fritextfältet.

Datainspektionen förutsätter att nämnden utfärdar skriftliga instruktioner till alla skolor som använder fritextfältet om vilka uppgifter som är relevanta att lämna i fritextfältet.

- 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 det bl.a. kan förekomma att uppgifter om att en elev är "sjukanmäld" eller frånvarande p.g.a. "läkar- och tandläkarbesök" behandlas genom de förvalda orsaksalternativen i frånvarorapporteringen i Skola24, utan att nämnden inhämtar uttryckligt samtycke till behandling av känsliga personuppgifter. En uppgift om att en elev är sjukanmäld eller t.ex. på läkarbesök är, alldeles oavsett om symtom eller diagnos anges, en känslig personuppgift i personuppgiftslagens mening.

Datainspektionen förutsätter att nämnden, om den vill fortsätta att behandla känsliga personuppgifter i Skola24, 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 personuppgifter; dessa kan exempelvis vara uppgifter om att en elev är sjuk eller på läkar- och tandläkarbesök. Vidare har framkommit att lärare och vårdnadshavare har åtkomst till Skola24 över Internet och att inloggningen sker med endast användarnamn och lösenord.

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

Datainspektionen förutsätter att nämnden vidtar tekniska åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av uppgifterna i Skola24 (d.v.s. 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 Skola24 sköts av Novasoftware samt att Tietoenator driftar Rexnet och att nämnden saknar personuppgiftsbiträdesavtal med företagen.

Datainspektionen förutsätter att nämnden ingår ett sådant 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 kännedom om och i så fall när personuppgifter gallras i Skola24, Rexnet och Extens.

Datainspektionen förutsätter att nämnden ta fram riktlinjer och rutiner för bevarande och gallring av personuppgifter i dessa IT-system, vilka även omfattar de behandlingar som personuppgiftsbiträden utför på nämndens uppdrag.

- Information till 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 självmant lämna den registrerade information om behandlingen av uppgifterna.

Vidare anges i 25 § första stycket PuL följande.

Information enligt 23 eller 24 § skall omfatta

- uppgift om den personuppgiftsansvariges identitet,*
- uppgift om ändamålen med behandlingen, och*
- 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, 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.

I ärendet har framkommit att elever och/eller vårdnadshavare inte får någon information om den personuppgiftsbehandling som sker i Skola24.

Datainspektionen förutsätter att nämnden fortsättningsvis ger vårdnadshavarna och eleverna fullständig information om den personuppgiftsbehandling som sker i Skola24.

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.

Patrik Sundström

Kopia till:

Personuppgiftsombudet Roland Andersson, Uppsala kommun, UTS
Kommunikation & IT, 753 75 UPPSALA