

Kommunstyrelsen i Stockholms stad
Stadshuset
Att: Agneta Herlin
105 35 Stockholm

Samråd om webbaserat verksamhetsstöd till Stockholms stads grundskolor

Frågeställning

Som personuppgiftsombud har du efterfrågat Datainspektionens vägledning i fråga om det webbaserade verksamhetsstödet för Stockholms stads (härefter: Staden) kommunala grundskolor, det s.k. Stockholms skolwebb (härefter SKW).

De frågor du ställt är sammanfattningsvis:

1. Krävs e-legitimation eller sms-inloggning för elever och vårdnadshavare vid inloggning över Internet i SKW?
2. Är det förenligt med PuL att möjliggöra ett fritextfält för kommentarer i samband med frånvaroregistrering?
3. Krävs det samtycke för behandlingen av känsliga personuppgifter i åtgärdsprogram och underlag för utvecklingssamtal?
4. Är det förenligt med PuL att möjliggöra en elevdagbok som innehåller känsliga personuppgifter?
5. Krävs det samtycke för överflyttningar av dokument när elever byter skola?
6. Datainspektionens synpunkter i övrigt värdesätts.

Datainspektionens vägledning

Inledningsvis vill Datainspektionen erinra om att det är den personuppgiftsansvariges uppgift att självständigt och på eget ansvar se till att behandlingen av personuppgifter följer personuppgiftslagen (PuL).

Datainspektionen vill inledningsvis också påpeka att behandling av personuppgifter i skolan har ett generellt stöd i 10 d § PuL. Av den bestämmelsen framgår att personuppgifter får behandlas utan den registrerades

samtycke om behandlingen är nödvändig för att en arbetsuppgift av allmänt intresse ska kunna utföras. Skolans fullgörande av sina arbetsuppgifter anses vara en sådan arbetsuppgift av allmänt intresse som avses i 10 d § PuL, se SOU 2003:103, *Sekretess i elevernas intresse - Dokumentation, samverkan och integritet i skolan*, sid. 199. En förutsättning är givetvis att uppgifterna behandlas i enlighet med personuppgiftslagens alla övriga bestämmelser, t.ex. 9 § om grundläggande krav vid behandling.

För känsliga personuppgifter gäller särskilda regler, vilket kommer att utvecklas i det som följer nedan.

Datainspektionen vill också fästa Stadens uppmärksamhet vid att uppgifter som läggs in i SKW kan bli allmänna handlingar som omfattas av offentlighetsprincipen och därmed kan behöva lämnas ut till den som så begär.

Sammanfattning av Datainspektionens bedömningar

Inloggning och åtkomst till känsliga eller på annat sätt integritetskänsliga personuppgifter över Internet kräver att starka autentiseringsåtgärder vidtas för att säkerställa mottagarens identitet.

För varje behandling av känsliga personuppgifter i fritextfält, i standardiserade kommentarer för frånvaroregistrering, i åtgärdsprogram, i underlag för utvecklingssamtal och i elevdagboken krävs samtycke. Detta gäller oavsett om vårdnadshavarna och eleverna ges åtkomst eller inte till uppgifterna efter inloggning över Internet.

Det är också viktigt att Staden tar hänsyn till vem som har personuppgiftsansvaret för skolornas personuppgiftsbehandlingar, till behovet av information till de registrerade eller deras vårdnadshavare, till att behandlingshistoriken sparas och till att personuppgifterna inte sparas längre än nödvändigt.

1. Säkerheten vid inloggning

Stadens fråga är om det ur ett säkerhetsperspektiv är godtagbart att inloggning i SKW kan ske över Internet för lärare, vårdnadshavare och elever med hjälp av endast ett lösenord, eller om det måste ställas krav på sms-kod till mobiltelefon, personnummer och lösenord vid inloggning över Internet. Staden har upplyst att man för elevernas inloggning inte anser sig kunna kräva sms-kod till mobiltelefon, eftersom det inte kan förutsättas att alla elever har en mobiltelefon.

Staden har lämnat följande redogörelse för hur sms-koden fungerar. Sms-koden är ett engångslösenord som skickas till användarens mobiltelefon och används för inloggning i SKW. På SKWs webbsida anger användaren sitt personnummer och lösenord för sitt konto. När användaren har verifierats som behörig, skickas ett engångslösenord till användarens mobiltelefonnummer som finns registrerat i Stadens IT-system. Därefter får användaren upp en ny sida där han eller hon anger sitt engångslösenord. Om engångslösenordet är riktigt kommer användaren till den tjänst i SKW som han eller hon har behörighet till.

1.2 Datainspektionens bedömning

1.2.1 Bestämmelser i PuL

Enligt 31 § PuL ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, kostnaden för åtgärderna, särskilda risker med behandlingen och hur pass känsliga uppgifterna är. Vid bedömning av hur pass känsliga uppgifterna är ska särskilt beaktas om personuppgifterna definieras som känsliga i PuL samt om de omfattas av tystnadsplikt eller sekretess enligt sekretesslagen (1980:100) eller annan lagstiftning.

1.2.2 Autentisering i SKW

Det är inte tillräckligt att enbart med användarnamn och lösenord autentisera användarna då de ansluter till SKW via Internet och tar del av personuppgifter som är känsliga enligt 13 § PuL eller på annat sätt integritetskänsliga.

Känsliga personuppgifter enligt PuL eller 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.

Behandlingen av personuppgifter i SKW uppfyller således inte säkerhetskraven i PuL beträffande känsliga eller andra integritetskänsliga personuppgifter, om dessa kommuniceras över Internet utan att tillräckliga åtgärder har vidtagits för att säkerställa mottagarens identitet.

Om däremot Staden vid inloggning över Internet förutom lösenord också kräver sms-kod till mobiltelefon samt personnummer, kan även känsliga eller andra integritetskänsliga personuppgifter kommuniceras över Internet. Detta gäller under förutsättning att uppgifterna även förses med krypteringsskydd vid överföringen, t.ex. med hjälp av SSL/TLS.

Om det inte anses möjligt att kräva sms-inloggning eller e-legitimation av elever när dessa loggar in i SKW via Internet (om det exempelvis inte kan förutsättas att samtliga elever äger mobiltelefoner eller de är för unga för att kunna komma ifråga för e-legitimation), anser Datainspektionen att elevernas åtkomst via Internet ska begränsas till enbart uppgifter som varken är känsliga enligt 13 § PuL eller på annat sätt integritetskänsliga.

När det gäller inloggning i SKW från interna nät, som Stadens administrativa nätverk och skoldatanätverk, ställer Datainspektionen inte motsvarande krav på stark autentisering med hjälp av e-legitimation, engångslösenord eller liknande. Detta gäller under förutsättning att kontrollen över det interna nätet i övrigt är säkerställd.

2. Fritextfält för frånvaroregistrering

Idag är det möjligt att göra anteckningar i fritextfältet för frånvaroregistrering i SKW. Denna möjlighet utnyttjas och det finns inga begränsningar eller riktlinjer för vad som får skrivas in i fritextfältet. Således kan det förekomma känsliga personuppgifter i fritextfältet.

Enligt Staden skulle ett alternativ till fritextfält vara att man fastslår ett begränsat antal standardiserade kommentarer till frånvaron.

2.1 *Datainspektionens bedömning*

2.1.1 *Bestämmelser i PuL*

Av de grundläggande kraven i 9 § PuL följer bl.a. att de personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålet med behandlingen samt att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Enligt 13 § PuL är det förbjudet att behandla s.k. känsliga personuppgifter. Med känsliga personuppgifter menas bl.a. sådana uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller personuppgifter som rör hälsa eller sexualliv. Av 15 § PuL framgår att känsliga personuppgifter får behandlas bl.a. om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen.

2.1.2 *Adekvata och relevanta personuppgifter*

PuLs krav på adekvans och relevans innebär att uppgifter som skrivs in i ett fritextfält för frånvaroregistrering endast får beröra frågor som skolan behöver i samband med att en elev är frånvarande.

En adekvat och relevant uppgift i fritextfältet skulle kunna vara uppgift att frånvaron har godkänts av vårdnadshavare eller lärare, eller att frånvaron är giltig av annat skäl. Däremot bör Staden överväga i vad mån uppgifter om läkarbesök och sjukdom är adekvata och relevanta, eftersom dessa uppgifter vanligen inte behövs för att kunna bedöma om frånvaron är giltig. En annan sak är att man inom skolhälsovården kan behandla uppgifter om vilken sjukdom en elev har eller om elevens läkarbesök.

Uppgift om skälen till giltig frånvaro, såsom besök hos skolhälsovården eller kurator kan i sig vara integritetskänsliga, även i förhållande till elevens vårdnadshavare. Skälen till elevens frånvaro kan även i vissa fall omfattas av sekretess gentemot vårdnadshavaren. Det sistnämnda är dock en fråga som regleras av bestämmelser i sekretesslagen och inte av bestämmelser i PuL.

Staden måste aktivt ta ställning till om det är nödvändigt, med hänsyn till ändamålet med behandlingen, att ha ett fritextfält där fritt valda kommentarer till frånvaron kan lämnas. Om staden bedömer att fritextfältet ska vara kvar måste staden utfärda skriftliga instruktioner till användarna om vilka uppgifter som är relevanta att lämna i fritextfältet och vilka sekretessregler som gäller.

Mot bakgrund av det sagda anser Datainspektionen att det föreslagna alternativet med en lösning där ett begränsat antal standardiserade kommentarer till frånvaron möjliggörs – i stället för ett fritextfält – ger Staden en bättre garanti för att inga inadekvata eller irrelevanta uppgifter behandlas.

2.1.3 Känsliga personuppgifter – krav på samtycke

Datainspektionen anser att Staden saknar stöd i PuL eller annan författning för att i samband med frånvaroregistrering utan samtycke automatiserat behandla känsliga personuppgifter.

Datainspektionen har tidigare uttryckt sin åsikt på denna punkt bl.a. i inspektionens rapport 2002:2 *Behandling av elevers personuppgifter i skolan*, sid. 8, där det sägs att samtycke krävs för att hälsouppgifter ska få behandlas för elevadministrativa ändamål.

Datainspektionens ståndpunkt har stöd i SOU 2003:103, sid. 201, där följande sägs. ”Gemensamt för de flesta fall då känsliga personuppgifter behandlas automatiserat inom ramen för det faktiska handlandet i skolverksamheten (undantaget skolhälsovården samt legitimerade psykologer och psykoterapeuter) är att det krävs samtycke från eleven eller, i förekommande fall, dennes vårdnadshavare. Utan ett sådant uttryckligt samtycke är det alltså normalt inte tillåtet att behandla uppgifterna automatiserat, även om det från skolans eller personalens synvinkel ter sig nödvändigt. Som exempel kan nämnas att det i dag krävs samtycke för att skolpersonalen i en frånvarojournal skall få anteckna orsaken till en elevs frånvaro, i den mån en sådan anteckning innebär att hälsouppgifter registreras.”

Mot bakgrund härav anser Datainspektionen att PuLs förbud mot behandling av känsliga personuppgifter utan samtycke innebär att Staden bör inhämta samtycke till att känsliga personuppgifter behandlas i samband med frånvaroregistreringen. Detta gäller oavsett om Staden väljer en lösning med fritextfält eller standardiserade kommentarer.

2.1.4 Vem kan samtycka?

Ett samtycke ska inhämtas från vårdnadshavarna i de fall det är fråga om barn som inte uppnått en sådan mognad att de själva kan tillgodogöra sig information om vad en behandling innebär. Barn under 15 år kan inte generellt sett anses ha nått en sådan mognad att de är kapabla att ta ställning i samtyckesfrågan i detta fall. För att samtycket ska vara giltigt krävs också att de som ska lämna samtycket får information om hur och varför personuppgifterna hanteras.

Samtycket ska vara frivilligt. Det innebär att en automatiserad personuppgiftsbehandling som kräver samtycke inte får vara skolans enda möjlighet att utföra den dokumentation om eleven som krävs i de författningar som reglerar skolans verksamhet, och inte får vara skolans enda kommunikationsväg med vårdnadshavarna.

Den information som ska lämnas i samband med att ett samtycke inhämtas ska enligt 25 § PuL innehålla uppgifter om följande.

- Vem som är personuppgiftsansvarig,
- ändamålet med behandlingen,
- vilka uppgifter som behandlas,
- hur länge uppgifterna sparas,
- vilka uppgifterna kan komma att lämnas ut till,
- att den registrerade har rätt att begära information om behandlingen av de personuppgifter som rör honom eller henne (registerutdrag) och
- att den registrerade har rätt att begära att felaktiga uppgifter ska rättas.

Om information enligt ovan lämnas till vårdnadshavarna, kan de vårdnadshavare som loggar in på SKW för att ta del av uppgifterna, anses ha lämnat sitt uttryckliga samtycke till behandlingen. Staden bör dock ta fram rutiner för på vilket sätt denna information ska lämnas till vårdnadshavarna.

Slutligen framgår av 12 § PuL att en vårdnadshavare eller elev som genom sitt samtycke har tillåtit behandling av känsliga personuppgifter, när som helst har rätt att återkalla samtycket. Sedan den personuppgiftsansvarige mottagit återkallelsen, får några ytterligare uppgifter om den registrerade inte samlas in eller annars behandlas. Behandlingen av redan insamlade uppgifter får trots återkallelsen fortsätta i enlighet med det ursprungligen lämnade samtycket, men uppgifterna får således inte t.ex. uppdateras eller kompletteras. (Prop. 1997/98:44, sid. 122)

I detta sammanhang vill Datainspektionen göra Staden uppmärksam på inspektionens informationsskrift *Samtycke enligt Personuppgiftslagen* (2007) och på inspektionens allmänna råd *Information till registrerade enligt personuppgiftslagen* (2000) som finns på www.datainspektionen.se.

2.1.5 Personuppgiftsansvaret

Vidare kan i sammanhanget påminnas om att personuppgiftsansvaret även för vårdnadshavarnas anteckningar i fritextfältet ligger på Staden (aktuell nämnd), och inte på vårdnadshavarna.

3. Känsliga personuppgifter i åtgärdsprogram osv.

Staden uppger att känsliga personuppgifter bedöms förekomma i åtgärdsprogram och i underlag för utvecklingssamtal.

3.1 Datainspektionens bedömning

3.1.1 Känsliga personuppgifter – krav på samtycke

Om Staden kommer att behandla personuppgifter, som enligt 13 § PuL är känsliga, i åtgärdsprogram och i underlag för utvecklingssamtal, bör samtycke inhämtas. Skälen för detta är samma som anges ovan punkt 2.1.3 under rubriken *Känsliga personuppgifter – krav på samtycke*.

Beträffande vem som kan lämna samtycke, hur samtycket ska lämnas, vilken information som ska ges till vårdnadshavarna eller eleven och vem som har personuppgiftsansvaret, se ovan punkterna 2.1.4 och 2.1.5.

3.1.2 Adekvata och relevanta uppgifter och rätt användare

Bestämmelser i PuL

Som redan nämnts under punkt 2.1.1, är det ett grundläggande krav vid all behandling av personuppgifter att personuppgifterna som behandlas är adekvata och relevanta i förhållande till de ändamål som har bestämts för behandlingen av personuppgifterna.

Andra grundläggande krav enligt 9 § PuL vid all behandling av personuppgifter, är att personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål, samt att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Adekvata och relevanta personuppgifter

I åtgärdsprogram och underlag för individuella utvecklingsplaner kan det förekomma personuppgifter som inte är känsliga i den mening som avses i 13 § PuL, men som ändå är att anse som integritetskänsliga. Exempelvis kan det röra sig om uppgifter om elevens sociala utveckling, dennes ogiltiga frånvaro eller om omdömen och värderande uppgifter. PuLs grundläggande krav på adekvans och relevans är av särskild vikt när det gäller behandling av integritetskänsliga personuppgifter.

Även om dessa slags uppgifter inte är känsliga uppgifter i personuppgiftslagens mening, är det ändå av vikt att sådana uppgifter utformas med respekt för elevernas personliga integritet.

Därför bör Staden utforma regler för vilka uppgifter som får förekomma i åtgärdsprogram och underlag för individuella utvecklingsplaner.

Rätt ändamål – rätt användare

De ovannämnda grundläggande kraven angående ändamålet med behandlingen, innebär att åtkomst till personuppgifterna inte bör ges till personer som inte behöver dem i sitt arbete. Om sådana personer tar del av uppgifterna, sker det nämligen i annat syfte än det professionella ändamål för vilket uppgifterna samlades in. PuLs grundläggande krav angående ändamålet med behandlingen är av särskild vikt när det gäller integritetskänsliga personuppgifter.

Därför är det troligtvis inte förenligt med kraven angående ändamålet med behandlingen, att göra elektroniskt lagrade integritetskänsliga uppgifter om elever tillgängliga för läsning av andra personer än dem som är berörda av uppgifterna. Berörda skulle exempelvis kunna vara eleven, vårdnadshavarna och lärare som skrivit in uppgifterna om den aktuella eleven.

Därför bör Staden utforma regler för vem som ska få åtkomst till åtgärdsprogram och underlag för individuella utvecklingsplaner, samt utforma system och rutiner för behörighetskontroll i enlighet med dessa regler.

Säkerhet

Vid utformning av säkerhet kring behandling av personuppgifter ska man bl.a. beakta de särskilda risker som finns med behandlingen av personuppgifterna (31 § första stycket c PuL personuppgiftslagen). I detta sammanhang vill Datainspektionen göra Staden uppmärksam på inspektionens allmänna råd *Säkerhet för personuppgifter* (1999) som finns på www.datainspektionen.se.

Sammanfattning – integritetskänsliga personuppgifter

Om Staden kommer att behandla integritetskänsliga personuppgifter i åtgärdsprogram och i underlag för utvecklingssamtal, bör Staden utforma regler för vilka uppgifter som får förekomma i dessa dokument, för vem som ska få åtkomst till dokumenten samt för de säkerhetsåtgärder som ska vidtas när dessa dokument används.

4. Elevdagboken

Det har framkommit att elevdagboken är tänkt att kunna innehålla känsliga personuppgifter i PuLs mening.

4.1 Datainspektionens bedömning

Eftersom Staden kommer att behandla personuppgifter som enligt 13 § PuL är känsliga i elevdagboken, bör samtycke inhämtas. Skälen för detta är samma som anges ovan punkt 2.1.3 under rubriken *Känsliga personuppgifter – krav på samtycke*.

Beträffande vem som kan lämna samtycke, hur samtycket ska lämnas, vilken information som ska ges till vårdnadshavarna eller eleven och vem som har personuppgiftsansvaret, se ovan punkterna 2.1.4 och 2.1.5.

Vidare måste Staden aktivt ta ställning till om det är nödvändigt, med hänsyn till kravet på adekvans och relevans samt ändamålet med behandlingen, att ha en elevdagbok där fritt valda anteckningar och synpunkter om eleven ska kunna skrivas in. Om Staden bedömer att elevdagboken ska införas måste Staden utfärda skriftliga instruktioner till användarna om vilka uppgifter som får skrivas in i elevdagboken och vilka sekretessregler som gäller.

5. Överflyttningar av dokument

Även överflyttning är en behandling av personuppgifter. Om det rör sig om känsliga personuppgifter som ska överflyttas, bör samtycke inhämtas även för just denna behandling. Det räcker med andra ord inte att samtycke till registrering har inhämtats från den överlämnande skolan; överflyttningen är en ny behandling som kräver uttryckligt samtycke. Samtycke till överflyttningen kan inhämtas samtidigt som samtycke till registreringen. Observera dock möjligheterna enligt 12 § PuL till återkallelse av samtycke.

Även själva överflyttningen av dokumenten måste ske på ett sätt som tillgodoser de krav på säkerhet som finns i 31 § PuL.

6. Övriga synpunkter

6.1 Personuppgiftsansvaret

I samrådsärendet har frågan väckts om skolornas rektorer kan vara personuppgiftsansvariga för den behandling som sker rörande deras respektive elever.

Datainspektionen vill i detta sammanhang framhålla följande. Den personuppgiftsansvarige ska se till att behandlingen av personuppgifter är laglig enligt PuL och har t.ex. ansvaret för informationssäkerheten och att de registrerade får den information de har rätt till. Personuppgiftsansvaret är straff- och skadeståndssanktionerat.

Personuppgiftsansvaret i en kommun ligger normalt hos de kommunala nämnder som är så självständiga att de är förvaltningsmyndigheter. En kommunal nämnd som är förvaltningsmyndighet är således vanligtvis personuppgiftsansvarig för de behandlingar av personuppgifter som nämnden har att utföra.

6.2 Information

Datainspektionen påminner om att även när det inte rör sig om behandling av känsliga personuppgifter för vilken samtycke krävs, måste de registrerade enligt 25 § personuppgiftslagen få information om att personuppgifter behandlas elektroniskt.

Beträffande en elev som fyllt 15 år bör informationen lämnas till eleven själv. Kan eleven inte tillgodogöra sig informationen, t.ex. då det är fråga om yngre barn, ska informationen istället lämnas till elevens vårdnadshavare.

6.3 Behandlingshistorik/loggar i SKW

Av Datainspektionens allmänna råd ”Säkerhet för personuppgifter” framgår bl.a. följande. För att åtkomsten ska kunna kontrolleras bör det, beroende på känsligheten hos personuppgifterna, finnas en behandlingshistorik som sparas en viss tid. Behandlingshistoriken bör normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Den bör vidare, beroende på känsligheten hos personuppgifterna, ange t.ex. läsning, ändring, utplåning eller kopiering av personuppgifter.

6.4 Gallring av personuppgifter i SKW

Till den del som dokumenten i SKW inte utgör allmänna handlingar som ska arkiveras och bevaras, får enligt 9 § PuL personuppgifterna inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Staden bör därför ta fram riktlinjer och rutiner för gallring av personuppgifter i SKW. Vägledning kan hämtas från Datainspektionen informationsskrift *Hur länge får personuppgifter bevaras?* (Nr 10, 2003) som finns på www.datainspektionen.se.

Beslut i detta ärende har – efter hörande av Datainspektionens styrelse – fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Leif Lindgren, datarådet Katja Isberg Amnäs, IT-säkerhetsspecialisten Magnus Bergström och juristen Erik Janzon, föredragande.

Göran Gräslund

Erik Janzon