



Checklista för skolor

Personuppgiftslagen (PuL) innehåller en rad bestämmelser som är viktiga att känna till för skolor som använder sig av IT-stöd i elevadministrationen. Datainspektionen har därför tagit fram denna checklista som kort sammanfattar några av de viktigaste punkterna som skolor måste tänka på när de behandlar personuppgifter. För enkelhetens skull talas här om "skolan" – men vanligtvis är det skolans huvudman, exempelvis en kommunal nämnd, ett bolag eller en förening, som har det yttersta ansvaret enligt personuppgiftslagen för hur personuppgifterna behandlas.

✓ Fritextfält

Om ett IT-system som behandlar personuppgifter innehåller ett fritextfält måste det finnas tydliga skriftliga instruktioner till användarna om vad som får skrivas i fritextfältet. Detta gäller oavsett om elever och vårdnadshavare eller bara lärare kan skriva i fritextfältet. Instruktionerna bör exempelvis ange hur värderande omdömen om eleven ska formuleras och att kränkande uttalanden inte är tillåtna.

✓ "Sjuk" som frånvaroorsak

Om det i samband med närvarorapportering registreras att eleven är sjuk måste vårdnadshavarens eller elevens samtycke till registreringen inhämtas. Detta gäller även om inga symtom eller diagnoser registreras. Utan samtycke får skolan bara registrera att eleven haft ogiltig frånvaro eller liknande. Det gäller dock inte för journalföring inom skolhälsovården där hälsouppgifter får registreras utan samtycke.

✓ Inloggning via Internet

Om skolans IT-system är tillgängligt via Internet, och systemet innehåller integritetskänsliga uppgifter, krävs det särskild god IT-säkerhet. Det innebär att skolan måste försäkra sig om att det verkligen är rätt personer som får åtkomst till uppgifterna och att överföringen sker på ett säkert sätt. Skolan måste använda sig av stark autentisering (exempelvis engångslösenord eller e-legitimation) och uppgifterna måste



förses med krypteringsskydd vid överföringen. Med integritetskänsliga uppgifter avses både känsliga uppgifter enligt 13 § personuppgiftslagen, men även uppgifter som omfattas av sekretess eller rör den enskildes personliga förhållanden.

✓ **Avtal med dina systemleverantörer**

Om en extern systemleverantör sköter driften och lagrar skolans personuppgifter krävs det att man ingår ett avtal. Leverantören anses vara skolans personuppgiftsbiträde. I avtalet ska det stå att leverantören får behandla personuppgifterna bara i enlighet med instruktioner från skolan och att leverantören är skyldig att upprätthålla god IT-säkerhet.

✓ **Hur länge får uppgifterna sparas?**

Det är viktigt att skolan bara sparar uppgifter som verkligen behövs för verksamheten och man bör därför ta fram skriftliga riktlinjer och rutiner för bevarande och gallring. Dessa bör även omfatta den behandling av personuppgifter som leverantörer (personuppgiftsbiträden) utför för skolans räkning. Det är skolans ansvar att se till att leverantörerna gallrar uppgifterna i rätt tid.

✓ **Information om vad skolan registrerar**

Skolorna måste informera elever eller vårdnadshavare om hur deras personuppgifter behandlas i IT-systemen. Skolan måste informera om vem som är ansvarig, vilka personuppgifter som samlas in, vad uppgifterna ska användas till samt att den registrerade har rätt att ansöka om information och begära rättelse av felaktiga uppgifter.

✓ **Får alla lärare läsa om alla elever?**

Bara den som behöver personuppgifterna i sitt arbete får ta del av dem. Det innebär att skolan måste införa begränsningar i läs- och skrivmöjligheterna i sina IT-system. Det är ofta lämpligt att både ha interna skriftliga regler i skolan för vilken anställd som får läsa vad och att införa tekniska begränsningar av läs- och skrivmöjligheterna.

✓ **Behörigheter inom skolhälsovården**

Inom skolhälsovården gäller mycket stränga krav på att bara den som deltar i vården av eleven eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården ska kunna ta del av uppgifter om en patient. Skolan har ansvaret för att det inte finns möjlighet för obehöriga att ta del av uppgifter i skolhälsovårdens elektroniska journalsystem. Exempelvis får det inte vara möjligt för en skolsköterska att ta del av uppgifter om en elev vid en annan skola (som hör till samma huvudman), om sköterskan inte är inblandad i vården av eleven.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.



Datainspektionen