

Förslag till anvisningar



Hantering av skyddade personuppgifter

inom stadens skolor

Bakgrund

Kommunfullmäktige har den 12 april 2010 antagit "Stadsövergripande policy om skyddade personuppgifter med riktlinjer till nämnder och bolag." Utbildningsförvaltningens anvisningar syftar till att komplettera den stadsövergripande policyn.

Skyddade personuppgifter

Enligt 22 kap. 1 § offentlighets- och sekretesslagen (2009:400, OSL) är uppgifter inom folkbokföringsverksamheten i regel offentliga. Sekretess gäller om det av särskild anledning kan antas att en person eller någon närstående, kan lida skada eller men om uppgiften om personen lämnas ut. Beroende på arten av hot finns tre grader av skyddade personuppgifter. Skyddade personuppgifter är Skatteverkets samlingsnamn för åtgärderna *sekretessmarkering*, *kvarskrivning* och *fingerade personuppgifter*.

Sekretessmarkering:

I de fall Skatteverket på förhand kan bedöma att utlämnande av uppgifter om en person kan orsaka personförföljelse eller annan skada kan en så kallad markering för särskild sekretessprövning (sekretessmarkering) sättas för personen i folkbokföringsdatabasen.

Det framgår inte vilken uppgift om personen i folkbokföringen som kan vara känslig. Markeringen fungerar som en varningssignal så att en noggrann prövning görs innan några uppgifter om personen lämnas ut.

Kvarskrivning:

Ett annat sätt att skydda personuppgifter i folkbokföringen är att genom beslut om kvarskrivning medge en person vid flyttning att vara folkbokförd på den gamla folkbokföringsorten i högst tre år. Kvarskrivning kräver särskilda skäl där det kan antas att personen kan bli utsatt för brott, förföljelser eller allvarliga trakasserier på annat sätt.

Fingerade personuppgifter:

Vid särskilt allvarliga hot kan en person medges att använda annan identitet. Beslut om detta meddelas av Stockholms tingsrätt efter ansökan hos Rikspolisstyrelsen.



Utbildningsförvaltningens anvisningar och handlingsplan

1. Skriftliga rutiner

Varje skola ska ha skriftliga rutiner för hantering av skyddade personuppgifter. Fastställda regler och rutiner krävs för att säkerställa att inga skyddade personuppgifter behandlas på ett sådant sätt att det innebär ökade risker och svåra konsekvenser för den enskilde. Vilka personuppgifter som särskilt måste skyddas kan givetvis variera från elev till elev. Det är därför viktigt att skolan i varje enskilt fall gör en bedömning om hur personuppgifterna ska behandlas. Vid behandlingen av elevers personuppgifter kan till exempel en uppgift om vilken skola eleven går i vara nog så viktigt att skydda som uppgifter om hemadress och telefonnummer. I denna bedömning kan man givetvis inhämta elevens och vårdnadshavarens inställning men det är alltid skolans ansvar att se till att behandlingen sker på ett säkert sätt.

Utbildningsförvaltningen rekommenderar skolverkets stödmaterial "Unga med skyddade personuppgifter"¹ samt Datainspektionens checklista "Skyddade personuppgifter i skolan"² som vägledning i hanteringen av elever med skyddade personuppgifter i skolan. En handlingsplan ska upprättas (exempel från Skolverket i bilaga 1).

2. Begränsa åtkomst av information och dokument

Vid hantering av personuppgifterna ska inte fler uppgifter behandlas än vad som behövs för ändamålet av behandlingen. För att i möjligaste mån minimera risken för spridning, bör man begränsa åtkomsten till känslig information och dokumentation kring elever med skyddade personuppgifter till ett fåtal personer samt förvara dokumentationen avskilt och på säker plats. För att minska riskerna för den enskilde ska man i varje enskilt fall noga analysera vilka personuppgifter som behöver registreras och kommuniceras. Skolan behöver ha rutiner för att rätt behörighet tilldelas och inaktuella behörigheter avslutas i stadens verksamhetssystem.

3. Information till personal

All personal som kommer i kontakt med skyddade personuppgifter behöver ha kännedom om skolans rutiner om hanteringen av elever med skyddade personuppgifter. Däribland ingår hantering av praktiska situationer samt hur man agerar i akuta situationer, exempelvis om personuppgifter röjs eller eleven utsätts för hot.

4. Kommunikation med personer med skyddade personuppgifter

Vid kommunikation använd säkra och med vårdnadshavare överrenskomna kommunikationskanaler. Kommunikation via e-post bör inte tillämpas i fråga om elever med skyddade personuppgifter vare sig inom eller mellan myndigheter. Den enskilde ska informeras om riskerna med att hantera elektroniska tjänster och e-post. Kommunikation med andra myndigheter per telefon kan vara möjlig efter motringning.

5. Kontroll

Det kan vara viktigt att i efterhand kunna spåra vilka som tagit del av uppgifter om en person med skyddade personuppgifter.

6. Stöd och vägledning

Vid behov av stöd och närmare information kontakta personuppgiftsombud eller systemförvaltare på utbildningsförvaltningen.

¹ <http://www.skolverket.se/publikationer?id=2507>

² <http://www.datainspektionen.se/Documents/faktablad-skyddade-skolor.pdf>