Riktlinjer för hantering av skyddade personuppgifter i skola och förskola

1 Inledning

Barn och elever med skyddade personuppgifter har samma rätt som andra unga till en utbildning av god kvalitet. Barnet eller eleven och dess vårdnadshavare ska också känna sig trygga med verksamheten och att deras uppgifter inte röjs.

Huvudmannen ansvarar för att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda alla personuppgifter som behandlas i organisationen, inte bara skyddade personuppgifter.[1]

En säker hantering av skyddade personuppgifter bygger på:

- Säkra IT-system
- Begränsad tillgång till skyddade personuppgifter
- Tydliga rutiner för hur personalen ska hantera skyddade personuppgifter

Det är rektor respektive förskolechef som ansvarar för att skyddade personuppgifter hanteras på ett korrekt sätt i verksamheten.

Orsaken till att barn och elever har skyddade personuppgifter varierar. Det är av stor vikt att verksamheterna kan garantera barns och elevers trygghet. Personal bör vara uppmärksam på om de behöver psykiatrisk behandling och i dessa fall förmedla kontakt med barn- och ungdomspsykiatrin.

Förskolans, skolans och fritidshemmens personal måste ge den trygghet som barnet eller eleven behöver för att kunna koncentrera sig på leken, fritidsverksamheten eller skolarbetet. Det kräver dels att skyddssystemen fungerar, dels att vuxna kan förmedla att de kan och vill skydda barnet/eleven.

All personal inom verksamheterna ska vara medveten om föreliggande riktlinjer samt rutiner[2] för hantering av skyddade personuppgifter inom skola och förskola för att förhindra att sekretesskyddad information röjs. Respektive chef ansvarar för att medarbetarna är informerade.

---

[1] Enheterna får inte använda nya system eller t.ex. molntjänster utan godkännande av huvudmannen.
2 Se särskilt dokument, Rutiner för hantering av skyddade personuppgifter i skola och förskola.

Bakomliggande lagstiftning
Detta styrdokument beslutas av utbildningsstyrelsen och beslutas med stöd av offentlighets- och sekretesslagen.'

Uppföljning och uppdatering
proVarmdo ansvarar för uppföljning och uppdatering av detta styrdokument.

1.1 Skyddade personuppgifter

Enligt offentlighet- och sekretesslagen[3] är folkbokföringsuppgifter i regel offentliga. Sekretess gäller om det finns anledning att anta att en person eller någon närstående kan lida skada eller men om uppgifter om personen lämnas ut. Skyddade personuppgifter är en samlingsrubrik som Skatteverket använder för olika skyddsåtgärder för personer som lever under hot om våld eller trakasserier. Det finns tre typer av skyddade personuppgifter, se 1.1.1, 1.1.2, och 1.1.3. nedan:

1.1.1 Sekretessmarkering

Om Skatteverket bedömer att ett utlämnande av personuppgifter kan orsaka personförföljelse eller annan skada kan de sätta en markering för särskild sekretessprövning (sekretessmarkering) i folkbokföringssystemet. Markeringen fungerar som en varningssignal så att en noggrann prövning görs innan uppgifter om personen lämnas ut. Markeringen gäller vanligen i ett år och kan förlängas. En sekretessmarkering omfattar alla personuppgifter.

1.1.2 Kvarskrivning

Kvarskrivning innebär att en person vid flyttning får fortsätta vara folkbokförd på den gamla orten. I dessa fall anges adressen till skattekontoret på den gamla orten som adress i folkbokföringsregistret. Den faktiska adressen förvaras manuellt hos Skatteverket. Kvarskrivning kombineras ofta med sekretessmarkering.

1.1.3 Fingerade personuppgifter

Vid allvarliga hot kan en person få använda en annan identitet, så kallade fingerade personuppgifter. Då får personen helt andra personuppgifter än de egna. Personuppgifterna meddelas av Stockholms tingsrätt efter ansökan hos Rikspolisstyrelsen. Kopplingen mellan den gamla och den nya identiteten finns bara hos Rikspolisstyrelsen.

2 Meddelande till kommunen om skyddade personuppgifter

Skatteverkets uppgifter från folkbokföringssystemet överförs varje vecka till kommunen. Det innebär att uppgifter om sekretessmarkering når myndigheterna inom en vecka efter att sekretessmarkering registrerats hos Skatteverket. Mottagande myndighet ansvarar för att ha rutiner för att underlätta hanteringen och minska risken för att sekretessmarkerade personuppgifter lämnas ut oavsiktligt.

[3] OSL 2009:400

Bakomliggande lagstiftning
Detta styrdokument beslutas av utbildningsstyrelsen och beslutas med stöd av offentlighets- och sekretesslagen.'

Uppföljning och uppdatering
proVarmdo ansvarar för uppföljning och uppdatering av detta styrdokument.

3 Beredskap, samverkan och säkerhetsrutiner

Förskolor och skolor ska ha en beredskap för att bemöta personer med skyddade personuppgifter. Personalen i verksamheterna behöver ha kunskap om riktlinjer och rutiner.

Verksamheternas IT-system ska vara säkra och fungera för alla barn och elever. Kraven på autentisering i elevadministrativa system är mycket viktiga och systemförvaltaren måste ha kunskap om vilka som har tillgång till systemet. Autentisering bör ske med e-legitimation eller genom användarnamn och engångslösenord.[4]

Huvudmannen ska ha gemensamma rutiner för hantering av skyddade personuppgifter. Rutinerna behöver utvärderas och förbättras regelbundet eftersom nya risksituationer kan tillkomma.

4 Samverkan

Det är viktigt med en fortsatt god samverkan mellan verksamheterna och socialkontoret. Socialkontoret kan erbjuda stödsamtal och stödverksamhet för både vuxna och barn. Det är även viktigt att samverka med polisen och att se till att barnet/eleven och vårdnadshavaren får hjälp att känna förtroende för polisen, som kan komma att behöva utföra skyddsarbete i vissa situationer. Det är bra att diskutera med polisen hur personalen ska göra om information om familjen har läckt ut eller om den som hotar kommer till verksamheten.

5 Utlämnande av sekretessuppgifter i särskilda fall

Frågan om sekretess mellan myndigheter kan lösas genom samtycke till att uppgifterna lämnas. En sekretessbelagd uppgift får också lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda (OSL 10 kap 27 §).

6 Vem ska få veta vad?

Risken att information läcker ut är mindre ju färre som är informerade. Men samtidigt ökar risken att ingen med tillräcklig information är tillgänglig om något akut händer. Säkerhet måste därför vägas mot tillgänglighet i varje enskilt fall. Olika personalkategorier kanske kan behöva olika mycket information. De personer som får informationen måste vara klara över sitt ansvar för att uppgifterna inte sprids.

Den som hotar kan använda ombud som släktingar och vänner för att få information eller

[4] Checklista för skolor, Datainspektionen 2008, se www.datainspektionen.se.

Bakomliggande lagstiftning
Detta styrdokument beslutas av utbildningsstyrelsen och beslutas med stöd av offentlighets- och sekretesslagen.'

Uppföljning och uppdatering
proVarmdo ansvarar för uppföljning och uppdatering av detta styrdokument.

kontakta barnet. Verksamheten måste vara uppmärksam på alla obehöriga som kommer eller som efterfrågar information.

Skolan/förskolan bör diskutera med vårdnadshavaren/barnet vad personalen ska svara om andra barn, elever eller föräldrar ställer frågor.

7 Rekommenderad läsning

Skolverket: Unga med skyddade personuppgifter, www.skolverket.se
Skatteverket: Information om skyddade personuppgifter på www.skatteverket.se

Bakomliggande lagstiftning
Detta styrdokument beslutas av utbildningsstyrelsen och beslutas med stöd av offentlighets- och sekretesslagen.'

Uppföljning och uppdatering
proVarmdo ansvarar för uppföljning och uppdatering av detta styrdokument.