

Rutiner för hantering av skyddade personuppgifter inom vuxenutbildningen i Ekerö kommun

Inledning

Personer som lever med skyddade personuppgifter gör det för att dom själva eller någon närstående är utsatta för någon form av hot. Vardagliga situationer kan därför bli komplicerade att hantera för denna grupp och om uppgifter kommer ut kan det få allvarliga konsekvenser. Det är därför viktigt att Barn- och utbildningsförvaltningen har rutiner för att hantera skyddade personuppgifter av olika slag. Rutinerna syftar således till att säkerställa att personal inom skola, och den kommunala förvaltningen hanterar elevers skyddade personuppgifter på ett rättssäkert och likvärdigt sätt.

Rutinerna innehåller information om

- vad som menas med skyddade personuppgifter,
- sekretess och allmän handling,
- ansökan om utbildning,
- hantering av IT-system,
- rutiner för enheterna samt
- information inför framtagandet av handlingsplanen

Det är rektor som ansvarar för att skyddade personuppgifter hanteras på ett korrekt sätt i verksamheten och elever får den utbildning och det stöd som de har rätt till. Hur det ska ske ska beskrivas i en handlingsplan som utformas för varje elev som har skyddade personuppgifter. Som stöd i detta arbete finns en checklista med saker som är viktiga att fundera kring för att hanteringen ska bli så bra som möjligt.

Skyddade personuppgifter

Skyddade personuppgifter är ett samlingsbegrepp som Skatteverket använder för tre olika typer av skyddsåtgärder när en person är utsatt för någon form av hot: sekretessmarkering, skyddad folkbokföring (tidigare kvarskrivning) och fingerade personuppgifter. I vardagligt tal kan även begreppet ”skyddad identitet” användas istället för skyddade personuppgifter.

Sekretessmarkering

I normalfallet är folkbokföringsuppgifter, som till exempel personnummer, namn och adress, offentliga vilket innebär att ”var och en” har rätt att ta del av dessa uppgifter. Genom att en sekretessmarkering förs in i folkbokföringssystemet blir uppgifterna skyddade, vilket innebär att varje myndighet noga måste pröva varje enskilt fall innan uppgifter lämnas ut. En sekretessmarkering gör det svårare för andra att ta del av uppgifterna. Sekretessmarkering är ingen absolut sekretess. Vilka uppgifter som är sekretessmarkerade framgår inte. I vardagligt tal kan begrepp som ”skyddad adress” eller ”skyddad identitet” förekomma när man talar om sekretessmarkering.

Skyddad folkbokföring (tidigare kvarskrivning)

Om det finns särskilda skäl, som till exempel att man blivit utsatt för brott, förföljelser eller andra allvarliga trakasserier, kan en person även få bli ”kvarskriven”. Det innebär att en person som flyttar behåller sin ”gamla adress”. Den nya bostadsadressen blir inte känd (faktisk adress förvaras manuellt på Skatteverket). Den nya adressen sprids då inte mellan myndigheter.

Fingerade personuppgifter

Person som är utsatt för särskilt allvarlig brottslighet där risk för liv hotas, kan fingerade personuppgifter användas som skydd. Det innebär att en person får en ”ny identitet” med till exempel nytt namn och nytt personnummer. Den gamla identiteten tas bort ur folkbokföringsregistret. Koppling mellan den gamla och nya identiteten finns endast hos polismyndigheten. Personer med fingerade personuppgifter behöver även flytta till ny hemlig ort.

Skydd via socialtjänsten

I vissa fall kan socialtjänsten meddela att en person behöver ha skydd för personuppgifter. Socialtjänsten gör en så kallad skyddsbedömning som betyder att de avgör om en anmälan kräver ett omedelbart skydd av den drabbade. När handläggare på stabsfunktionen får informationen om skyddsbedömningen så spärras personens personuppgifter i alla system. Handläggare agerar utifrån Socialtjänstens och klientens önskemål därefter i informationsbyte.

Bestämmelser om sekretess och hantering av förfrågan om allmän handling

Sekretessbestämmelser för utbildningsområdet kan skydda namn, adress och andra personuppgifter. Olika sekretessbestämmelser gäller för olika verksamheter inom utbildningsområdet.

Sekretess gäller i förskoleklass, grund- och grundsärskolan och gymnasie- och gymnasiesärskolan och vuxenutbildning för uppgift om en enskilds identitet, adress och andra liknande uppgifter om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs (23 kap. 2 § tredje stycket OSL). Sekretessen omfattar alltså elevens och namn och adresser och även andra folkbokföringsuppgifter. Särskild anledning till sekretess kan i detta sammanhang vara att personen ifråga har ett beslut om kvarskrivning eller sekretessmarkering.

Förfrågan om allmän handling

Vid förfrågningar om att få ta del av allmänna handlingar ska sekretessmarkering och skyddad folkbokföring fungera som en varningssignal. Skatteverket har gjort bedömningen att det finns en risk att eleven eller dess närstående riskerar att förföljas eller trakasseras på annat sätt. En sekretessmarkering eller skyddad folkbokföring ska därför ingå som en del av underlaget vid bedömningen om en handling ska lämnas ut.

Viktigt att tänka på är att oavsett om en sekretessmarkering eller annan skyddsåtgärd finns så ska verksamheten göra en egen prövning vid en begäran om utlämnande. Det kan vara så att personalen har sådan information om ett elevens förhållande att det finns anledning att anta ett eleven eller närstående kan lida men om uppgiften utlämnas. Det innebär att skolmyndigheten efter en prövning kan sätta sin egen sekretessmarkering.

Hur hanteras ansökan, beslut och erbjudande om plats i och skola?

Ansökan om plats i plats i skola görs i vanliga fall via kommunens självbetjäningstjänst "Självservice" som nås via kommunens hemsida. Personer med någon form av skyddade uppgifter ska inte använda Självservice genom kommunens hemsida. De ska istället per telefon ta kontakt med Studie och yrkesvägledare på Ekerö vuxenutbildning. När eleven söker skola så ska kommunen uppmärksammas om vilken typ av skyddade personuppgifter som är aktuella. Förvaltningen hanterar då ansökan utanför systemet i dialog med eleven och kommer också överens om hur den fortsatta kontakten ska ske.

Ansvarig personal på Ekerö vuxenutbildning ska i samband med start i verksamheten skyndsamt kalla till ett planeringsmöte. Ett planeringsmöte ska även hållas när elever som

redan befinner sig i verksamheten får skyddade personuppgifter. På mötet tas en handlingsplan fram för hur hanteringen av skyddade personuppgifter är tänkt att fungera i den aktuella verksamheten. Planen utformas i samverkan med personal och elev.

Hur ska skyddade personuppgifter hanteras på enheterna?

Planeringsmöte och handlingsplan

Om en elev har någon form av skyddade personuppgifter ska ett planeringsmöte genomföras med eleven om det anses lämpligt. Även i de fall verksamheten får information om skyddade personuppgifter när en elev redan är inskriven i verksamheten ska ett planeringsmöte genomföras. Det är viktigt att verksamheten bestämmer vem som ansvarar för samtalet och att den personen får stöd och vägledning kring hanteringen av skyddade personuppgifter.

Syftet med samtalet är att klargöra hur elevens situation ser ut och att utforma en handlingsplan där man tar ställning till frågor som till exempel överlämning till andra utbildningsanordnare. Det är viktigt att man på enheten funderar kring de olika avsnitten i handlingsplanen och olika lösningar redan innan planeringsmötet. Kontakta gärna personal på förvaltningen för stöd och råd. Använd denna rutin som stöd när ni tar fram handlingsplanen, se närmare under rubriken Att tänka på vid framtagandet av handlingsplanen.

Hantering av handlingar rörande skyddade personuppgifter

Den dokumentation som finns gällande elev med skyddade personuppgifter (om det inte kan hanteras digitalt) ska finnas i en pärm inlåst hos skoladministratör med särskilt ansvar för skyddade personuppgifter. Bara rektor, studie och yrkesvägledare och skoladministratör bör ha tillgång till den. Handlingsplanen och all övrig dokumentation ska alltså enbart finnas in denna pärm. Utskrift av t.ex. betyg görs också manuellt enligt överenskommelse med elev. Vid arkivering läggs handlingarna i en akt som tydligt märks med röd, stor text: "Skyddad identitet".

Att tänka på vid framtagandet av handlingsplanen

Betygsdokument

Om en elevs personnummer inte ska hanteras i kommunens digitala system för betygsshantering, ska varje skola ha en rutin för att hantera detta manuellt.

Telefonkontakter

Kom ihåg att telefonkontakter kan innebära en säkerhetsrisk eftersom det inte alltid går att identifiera den som ringer. För att inte riskera att skyddade uppgifter lämnas ut kan ni komma överens om ett kodord eller ett annat säkert sätt som eleven kan identifiera sig på vid telefonkontakt.

Vem ska få veta vad?

Ju färre som är informerade desto mindre risk att information läcker ut. Men då ökar också risken att ingen av dem är närvarande när en akut situation uppstår. Säkerheten måste därför vägas mot tillgängligheten och det är något som måste diskuteras i varje enskilt fall. Ibland kanske olika personalkategorier ska få olika mycket information. Alla behöver nödvändigtvis inte veta allt. Att få veta vem som hotar är sällan viktigt. Dels är det ju ofta inte en utan flera personer, dels kan den som hotar använda ombud som släktingar eller vänner för att få ut information eller för att komma i kontakt. Skolan måste vara uppmärksam på alla obehöriga som kommer dit. Det är också viktigt att diskutera med eleven vad personalen ska svara om andra elever eller ställer frågor.

Som alltid gäller att aldrig samla in fler personuppgifter än nödvändigt med hänsyn till ändamålet med behandlingen.

Internet och IT-system

Det är viktigt att diskutera med eleven hur de kan använda nätet säkrare. Grundregeln är att skolan inte ska publicera namn, bilder eller andra personuppgifter på websidor, bloggar, Facebook eller liknande forum. Det är också viktigt att se över hur kommunen/skolans system för kommunikation med elever ska kunna skyddas från intrång av utomstående. Det gynnar inte bara elever med skyddade personuppgifter utan alla. Ett sätt att skydda uppgifter är genom att låta uppgifterna om en person bara vara tillgängliga för exempelvis skolans rektor. De personer som får tillgång till uppgifterna måste hantera dem med försiktighet och på ett sätt så att de inte sprids.

E-postadresser

Om eleven ska ges en e-postadress, för att kunna få personlig information från verksamheten och skicka e-post till andra inom eller utanför skolan, är det viktigt att diskutera med vilket namn. Adressen ska inte gå att spåra. Hemadress eller telefonnummer behöver inte finnas med i epostsystemet eftersom det ökar risken att uppgifterna kan hämtas därifrån av någon.

Det är också viktigt att endast personer med inloggning i systemet kan söka efter användare.

Namn på listor och arbeten

Det är viktigt att tex listor och annan dokumentation med namn eller andra personuppgifter hålls inlåst och bara tas fram när ni behöver använda dem. Begränsa antalet papperskopior så att ni har kontroll över hur många kopior ni har och vilka som har tillgång till dessa.

Beredskap för akuta situationer

Om de skyddade personuppgifterna läcker ut måste ni snabbt samråda med eleven om vad ni kan göra för att minimera skadan. Kan ni göra något för att rätta till misstaget? Går det att täta läckor som uppstått? Bör ni kontakta polisen? Måste familjen flytta och ska ni kontakta socialtjänsten? Det är bara eleven som kan avgöra hur allvarlig situationen är och måste därför kontaktas så fort som möjligt.

Eleven måste också avgöra om han eller hon vill bli kontaktad när någon begärt ut uppgifter även om personalen inte lämnat ut den. Informera även förvaltningen (Staben) om personuppgifter läckt ut, då kan rutinerna utvärderas.

Sekretessmarkering tillkommer eller försvinner

Vi har ingen möjlighet till bevakning av detta. Ansvar för att informera om nya förhållanden måste därför ligga på berörd elev.

Samverkan med andra förvaltningar eller myndigheter

För att lösa frågor om sekretess mellan myndigheter kan ni i första hand fråga eleven, om samtycke till att uppgifterna lämnas. Dessutom innehåller offentlighets- och sekretesslagen en så kallad generalklausul. I många fall kan myndigheter och huvudmän samarbeta utan att behöva avslöja elevens identitet.

En säkerhetsrisk vad gäller personer med skyddade personuppgifter är när uppgifterna måste föras över från en kommun till en annan myndighet eller mellan en fristående huvudman och en kommun. Det är viktigt att inte lämna fler uppgifter än nödvändigt i kontakten med andra kommuner. I många fall kan ni lösa kommunikationen genom att inte använda brevpapper eller annat som avslöjar vilken kommun personen vistas i och genom att den tidigare kommunen skickar svaret via Skatteverkets postförmedling.

Om man måste lämna uppgifter mellan kommuner eller annan huvudman är det viktigt att den kommun som lämnar uppgifter uppmärksammar den andra på att uppgifterna i den avlämnande kommunen kan omfattas av sekretess.

Rensning av fiktiva personnummer elever som flyttat, sluta eller skydd upphör.

Om en elev finns i systemet med sina riktiga uppgifter kan den fiktiva eleven rensas bort (dock går det inte att ta bort den fiktiva personen ur systemet). Rensa även gamla ej aktuella handlingsplaner. Finns eleven inte med i systemet så måste dokumentationen finnas kvar för historik.

Postförmedling

Skatteverket kan förmedla post till personer med skyddade personuppgifter. Det finns särskilda rutiner för postförmedling som hanterar posten.

Gör följande med den post som du vill att Skatteverkets postförmedlingsservice ska förmedla:

- Det brev som ska förmedlas ska läggas i ett slutet kuvert. Kuvertet ska ha uppgift om avsändaradress så att Skatteverket kan returnera försändelsen om de inte kan nå mottagaren.
- På kuvertet ska du skriva mottagarens personnummer och, om möjligt, mottagarens full
- Du ska sedan lägga kuvertet i ett ytterkuvert som sänds till post-förmedlingsadress. Flera försändelser kan givetvis läggas i samma ytterkuvert. All din förmedlingspost kan sändas till samma postförmedlingsadress.
- Posten kommer att förmedlas till mottagaren oavsett var mottagaren bor.

Förmedlingsadress

Skatteverket Förmedlingsuppdrag

Box 2820

403 20 GÖTEBORG