MORA KOMMUN

RIKTLINJE
SKYDDADE PERSONUPPGIFTER

Riktlinje skyddade personuppgifter

Fastställd	Kommunfullmäktige 2019-11-25 § 117
Reviderad	-
Produktion	Kommunstyrelseförvaltningen
Dnr	2019/00419 00x

Innehållsförteckning

1. Inledning

Människor som är utsatta för hot eller riskerar att utsättas för brott, förföljelser eller allvarliga trakasserier kan få beslut från skatteverket att deras uppgifter ska skyddas. Skatteverkets samlingsrubrik är *skyddade personuppgifter*.

För att öka tryggheten för personer med skyddade personuppgifter inom kommunens verksamhetsområden har den här riktlinjen tagits fram som en vägledning. Alla verksamheter i kommunen omfattas av riktlinjen och den ska kompletteras med särskilda lokala instruktioner, checklistor, rutiner och samtalsguider.

2. Olika nivåer av skyddade personuppgifter

Det finns tre nivåer av skyddade personuppgifter: sekretessmarkering, skyddad folkbokföring (tidigare kvarskrivning) och fingerade personuppgifter. De två första beslutas av skatteverket och den tredje av tingsrätt. Riktlinjen gäller de två första nivåerna eftersom den tredje är fingerade nya personuppgifter. Vid fingerade personuppgifter känner vi inte till den tidigare identiteten och kan inte se att den nuvarande är en ny fingerad identitet.

Sekretessmarkering

Skatteverket för in en markering vid personuppgifterna som anger att ingen får lämna ut uppgifterna utan tillstånd och säkerhetskontroll. Markeringen ska fungera som en varningssignal om behovet av att göra en noggrann skadeprövning enligt 22 kap. 1 § offentlighets- och sekretesslagen (OSL) när någon begär att få ut en uppgift. Detta är den vanligaste typen av skyddade personuppgifter.

Vid en sekretessmarkering framgår det inte vilken uppgift om personen som ska skyddas. Adress är i regel den uppgift som är mest skyddsvärd, men det finns även andra uppgifter inom folkbokföringen som kan behöva skyddas, som det gamla personnumret för den som ändrat juridiskt kön eller namn för den som gjort ett namnbyte för att stärka sitt skydd.

Det kan också vara en berörd persons familj som behöver skydd, så även anhörigas uppgifter kan behöva skyddas.

Skyddad folkbokföring

Registreras när hotbilden mot en person är mycket stark och personen har skyddad folkbokföring enligt 16 § folkbokföringslagen (FOL).

Uppgifter om den som har skyddad folkbokföring ska normalt sett inte lämnas ut.

Personen står *kvarskriven* på den gamla orten när man flyttar. Den nya adressen förs aldrig in i folkbokföringen och lämnas inte ut till andra myndigheter. Personen är alltså folkbokförd på annan ort än där man är bosatt men med utökade möjligheter. Personen kan vara folkbokförd antingen på den gamla folkbokföringsorten vid flytt eller på en annan ort om det bedöms ge bättre skydd. Skyddad folkbokföring kan även medges till familjemedlem som är bosatt tillsammans med den utsatta personen och skyddet kan medges på obestämd tid.

3. Hantering av skyddade personuppgifter generellt i kommunen

Skyddade personuppgifter ska hanteras med mycket stor försiktighet. Det finns ett ansvar hos den enskilde att upplysa om att man har skyddade personuppgifter då det inte åligger en myndighet att utan anledning kontrollera det i folkbokföringen.

Markering för skyddad folkbokföring och sekretessmarkering, aviseras från Skatteverket till andra myndigheter. Mottagaren väljer vilket som är det lämpligaste sättet att hantera uppgifterna i sina verksamhetssystem. Olika system hanterar det på olika vis.

Verksamheterna i kommunen behandlar olika personuppgifter för att fullgöra sina uppdrag. Genom en riskanalys kan man klarlägga hur uppgifter om en person med skyddade personuppgifter ska behandlas i verksamheten. Man bör göra en översyn av vilken information man måste ha med i ansökningar, beslut, protokoll, klasslistor och andra handlingar för att undvika att få in skyddade personuppgifter.

Om skyddsbehovet kräver det ska ett fingerat namn användas i verksamhetens system, där det är möjligt. Utgångspunkt är den enskildes önskemål men verksamheten som ska behandla personuppgifterna ska förklara vad de olika alternativen innebär – eget namn eller fingerat namn. I vissa system måste det rätta namnet framgå.

Begäran om utlämnande av handling

Sekretessmarkering – markeringen är inte ett beslut om sekretess utan endast en varningssignal att göra en noggrann skadeprövning enligt 22 kap. 1 § OSL. Om myndigheten bedömer att uppgifter i handlingen omfattas av sekretess ska myndigheten fråga vem som begär ut handlingen för att kunna bedöma om handlingen kan lämnas ut till just den aktuella mottagaren.

Markering för *skyddad folkbokföring* – uppgifter om den som har skyddad folkbokföring ska normalt sett inte lämnas ut.

Behöriga personer

Risken att uppgifterna felaktigt lämnas ut ökar med antalet handläggare som kan ta del av uppgifterna. Kretsen av personer som har behörigheten att ta del av skyddade personuppgifter ska begränsas så långt som möjligt.

IT-stöd

Behandling av skyddade personuppgifter i IT-system ska följa Skatteverkets vägledning för hantering av skyddade personuppgifter.

Det ska på ett tydligt och enhetligt sätt framgå för de användare som har behörighet till skyddade personuppgifter att uppgifterna är markerade för skyddad folkbokföring eller har sekretessmarkering, både i IT-system och på utskrifter.

Åtkomst till skyddade personuppgifter ska loggas för att i efterhand kunna kontrollera vilka som tagit del av uppgifterna.

Ansvar för medarbetarnas kunskap i ämnet

Varje verksamhet bör utse en särskild person som har ansvar för att rutiner och regler för hantering av skyddade personuppgifter följs.

Verksamheten ansvarar för att medarbetare har goda kunskaper om systemet med skyddade personuppgifter.

Verksamheten ansvarar för att medarbetare har goda kunskaper om sekretessbestämmelser i sin verksamhet.

Kommunikation med person med skyddade personuppgifter

Man kan vända sig till den enskilde eller andra myndigheter endast via en säker kommunikationskanal. Som säkra kommunikationskanaler rekommenderar skatteverket brev, elektronisk kommunikation med hjälp av en elektronisk legitimation och personligt besök av den enskilde om han eller hon har legitimerat sig. Kommunikation via e-post ska inte tillämpas i fråga om uppgifter som omfattas av sekretess, vare sig inom eller mellan myndigheter.

Kommunikation med andra myndigheter per telefon kan vara möjlig efter att man kontrollerat att uppringaren är den man utger sig för att vara. Det kan ske genom återuppringning till den myndighetens officiella telefonnummer (s.k. motringning).

Om man inte har någon adressuppgift i verksamheten ska Skatteverkets förmedlingstjänst användas. Information finns på Skatteverkets webbplats.

Personer med skyddade personuppgifter ska informeras om vikten av att inte i onödan lämna ut uppgifter om sig själva.

4. Hantering av skyddade personuppgifter hos medarbetare

Vid rekrytering och vid avisering till arbetsgivaren

Rekommendationen är att personer med skyddade personuppgifter inte använder kommunens rekryteringssystem för sin ansökan. För att man i systemet ska se att personen sökt läggs en manuell ansökan upp (av chef/HR) där fiktiva personuppgifter anges och personligt brev/cv utelämnas om det behövs.

Personer som får skyddade personuppgifter får ett skriftligt beslut. Beslutet visas för anställande chef, som meddelar lönechefen. Kontakt mellan medarbetarens chef och lönechef görs i första hand via telefon eller i slutna kuvert.

Ett samtal ska hållas för att reda ut praktiska frågor.

Personalakten förvaras inlåst endast tillgänglig för vissa anställda på löneenheten. För att inte uppgifter ska lämnas ut av misstag görs en tydlig markering om att medarbetaren har skyddade personuppgifter.

IT-system i arbetet

Arbetsgivaren och arbetstagaren går igenom vilka system som är nödvändiga för att utföra arbetsuppgifterna. Om skyddsbehovet kräver det ska ett fingerat namn användas där det är möjligt, som t ex användarnamn, e-post. Utgångspunkt är den enskildes önskemål men arbetsgivaren behöver förklara vad de olika alternativen innebär – eget namn eller fingerat namn. I vissa system måste arbetstagarens rätta namn framgå.

Viktiga saker att tänka på

- Vilka som ska informeras om att personen har skyddade personuppgifter och vilken information de ska få.
- I det inledande samtalet ska det klargöras hur medarbetare ska agera om någon frågar om personen med skyddade personuppgifter.
- I samtalet ska klargöras vad som ska hända om personuppgifter lämnas ut av misstag. Ska personen meddelas och vem ska göra det? Hur kan skadan minimeras?
- Ha en uppdaterad beskrivning av hotbild och konsekvenser för arbetsplatsen.
- Se till att arbetstagaren med skyddade personuppgifter samt övriga på arbetsplatsen som kan känna oro, får det stöd de behöver.

5. Hantering av skyddade personuppgifter inom utbildning

Nedan angivna term ”skola” gäller för- och grundskola, barnomsorg, kulturskola, gymnasium, vuxenutbildning och term ”elev” alla deltagare i beskrivna skolformer. Skolverket har gett ut ett särskilt stödmaterial med råd.

Vid inskrivning, avisering till skolan

Elev/vårdnadshavare ska själv upplysa rektor om att personuppgifterna är skyddade och ska även upplysa om skyddet ändras.

Personer som får skyddade personuppgifter får ett skriftligt beslut. Beslutet visas upp för rektor, som ansvarar för att uppgifterna hanteras på ett korrekt sätt i verksamheten.

Ett inledande samtal ska hållas där formerna för samarbetet mellan vårdnadshavaren, eleven och personalen diskuteras. Varje familjs situation är unik och utgångspunkten vid samtalet ska därför vara vårdnadshavarens och elevens önskemål.

Rektor ansvarar för att informationen når den personal som överenskommits i samtalet.

Rektor ansvarar för att informera berörd personal om sekretess och tystnadsplikt

IT-system i skolan

Om skyddsbehovet kräver det, ska ett fingerat namn användas där det är möjligt, som t ex i användarnamn och e-post. Utgångspunkt är vårdnadshavaren och elevens önskemål. I vissa system måste elevens rätta namn framgå. Rektor förklarar vad de olika alternativen innebär – eget namn, fingerat namn, inget namn. Vårdnadshavare eller myndig elev tar ställning.

Viktiga saker att tänka på

- Vilka som ska informeras om att personen har skyddade personuppgifter, vilken information de ska få och vad de olika alternativen innebär. Vårdnadshavare/myndig elev tar ställning.
- Hur kontakten mellan skolan och hemmet ska se ut. Skolan bör kunna presentera alternativ och redogöra för dessa, t ex vid frånvaro. Vårdnadshavare/myndig elev tar ställning.
- Hur skolan ska svara om någon ringer eller kommer till skolan och frågar efter eleven. Vid inkommande telefonsamtal ska skolan försäkra sig om att den som ringer är den man utger sig för att vara. Om det inte är möjligt att ringa tillbaka på ett känt nummer (motringning) ska besked lämnas postledes.
- Hur skolan ska agera om något inträffar. Det ska vara tydligt vem som ska kontaktas om något inträffar. Även hur denna kontakt ska se ut och hur ska den gå till. Gör iakttagelser som kan vara till hjälp för polisen, om något inträffar. Påminn om att det är av yttersta vikt att skolan meddelas om eleven inte kommer till skolan.
- Informera vårdnadshavare/myndig elev att andra i skolan kan komma att ställa frågor så att eleven är förberedd på hur det ska bemötas.
- Informera personalen om vad det innebär om personal från skolan ska närvara vid en eventuell rättegång. Risken är då stor att orten, skolan röjs.
- Elever med skyddade personuppgifter som inte valt fingerat namn bör inte
    - Finnas med i skolkatalogen.
    - Finnas med på Internet med bilder/namn.
    - Finnas med på klasslistor.

  Vårdnadshavare/myndig elev tar ställning.

6. Hantering av skyddade personuppgifter inom vård, stöd, sysselsättning och social omsorg

Det är viktigt att socialtjänst har beredskap för att möta och hjälpa personer med skyddade personuppgifter. Det kan handla om checklistor för säkerhetsåtgärder eller att ha särskilda tekniska lösningar i dokumentationssystemen. I Socialstyrelsens särskilda föreskrifter och allmänna råd om dokumentation i verksamhet som bedrivs med stöd av SoL, LVU, LVM och LSS[1] finns vidare regler om dokumentation som rör personer med skyddade personuppgifter.

Det är viktigt att nämnder kan hantera utredningar på ett säkert sätt om ett barn eller någon av vårdnadshavarna har skyddade personuppgifter.

Det råder stark sekretess kring personuppgifter inom området, vilket gör att det sällan lämnas ut uppgifter till någon annan än den som det berör.

Första kontakten med brukare/klient/kund

Den enskilde ska själv informera verksamheten om att personuppgifterna är skyddade och ska även upplysa om skyddet blir ändrat.

Vid den första kontakten ska ett samtal hållas för att diskutera formerna för samarbetet mellan den enskilde och kommunen. I vissa fall behöver samtalet föras med närstående och/eller god man. En checklista ska finnas som gås igenom vid samtalet.

Varje individs situation är unik och utgångspunkten vid samtalet ska därför vara den enskildes behov.

Journalföring enligt hälso- och sjukvårdslagen (HSL)

Vårdgivaren ska säkerställa att det är möjligt att föra *patientjournal* om

1. en patients identitet inte kan fastställas. Patienten läggs in med ett påhittat personnummer. I andra hand förs journal på papper.

2. en patient saknar svenskt personnummer. Patienten läggs in med ett påhittat personnummer. I andra hand förs journal på papper

3. en patient har skyddade personuppgifter.

Har patienten kraftigare skydd ska övervägande ske om journal ska föras **manuellt** efter samråd med patienten, som ska bli informerad om konsekvenserna av att ha en pappersjournal. Lokala rutiner krävs för att hantera en pappersbaserad journal.

Alternativt erhålls ett påhittat personnummer som enbart hanteras av en snäv krets behörig personal. I frågor som rör punkt 1–3 och i synnerhet punkt tre om skyddade personuppgifter ska alltid medicinskt ansvarig sjuksköterska (MAS) eller verksamhetschef HSL och skatteverket kontaktas för bedömning om hantering.

Hantering inom verksamheten för ensamkommande barn

Inom verksamheten för ensamkommande barn råder också stark sekretess för personuppgifter vilket gör att det sällan lämnas ut uppgifter till någon annan än den som det berör.

I hanteringen i verksamhetssystemet används samma rutiner som inom övriga socialförvaltningen. För personer med skyddade personuppgifter läggs inga adresser in i systemet utan pappersakter förvaras inlåsta endast tillgängliga för vissa anställda.

[1] SoL-socialtjänstlagen, LVU-lagen om vård av unga, LVM-lagen om vård av missbrukare, LSS-lagen om stöd och service för funktionshindrade

Hantering inom individ- och familjeomsorgen (IFO)

Personalen på IFO arbetar utifrån kompletterande rutiner kring hantering av skyddade personuppgifter för myndighetsutövningen. Där ställs olika frågor till klienten utifrån dennes behov som till exempel hur man hanterar post och kontakter med klienter.

För att säkerställa att alla uppgifter som rör personer med skyddade personuppgifter gås igenom ska enhetens egna rutiner följas.

I hanteringen i verksamhetssystemet används samma rutiner som inom övriga socialförvaltningen. För personer med skyddade personuppgifter läggs inga adresser in i systemet utan pappersakter förvaras inlåsta, endast tillgängliga för vissa anställda.

Viktiga saker att tänka på

- Diskutera hur långt verksamhetens ansvar sträcker sig och var den enskildes ansvar tar vid.
- Vilka som ska informeras om att personen har skyddade personuppgifter och vilken information de ska få.
- Diskutera hur den löpande kontakten mellan den enskilde och verksamheten ska gå till.
- Om det finns särskilda risker som verksamheten ska beakta, något som personalen ska vara särskilt uppmärksamma på.