Promemoria

Skyddade personuppgifter – myndigheters hantering

ES2023-12

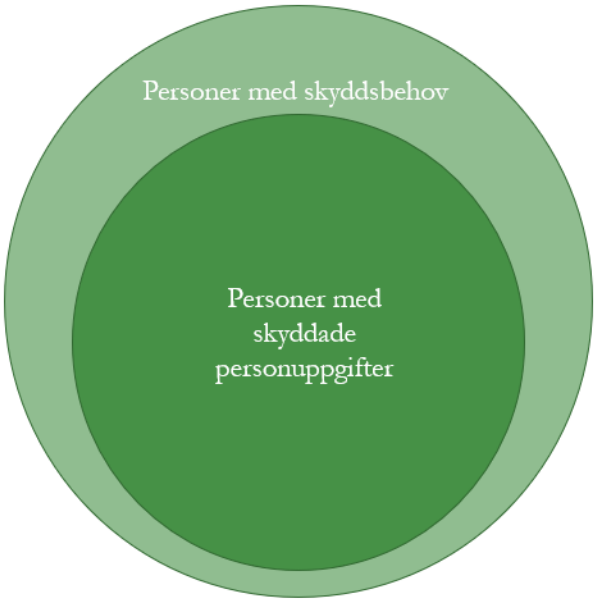
December 2023

Innehåll

1. Inledning

Det finns enskilda som lever med en hotbild riktad mot sig och därmed har ett *skyddsbehov*. Personer som är utsatta för hot kan i vissa fall få *skyddade personuppgifter*, dvs. omfattas av skyddsåtgärderna i folkbokföringen. Det innebär att uppgifter som vanligen är offentliga i det svenska folkbokföringsregistret kan skyddas, exempelvis namn och adress.

I figuren nedan illustreras att det finns personer med ett skyddsbehov, men som inte har skyddade personuppgifter. Dessa personer har ofta inte samma skydd i lagstiftningen som personer med skyddade personuppgifter.



Det är en angelägen uppgift för samhället att öka tryggheten och ge skydd åt de personer som lever i rädsla på grund av att de riskerar att utsättas för brott, förföljelser eller allvarliga trakasserier på annat sätt.[1] Det ställs stora krav på hur myndigheter hanterar uppgifter om dessa personer i verksamheten.

Myndigheter förväntar sig att kunna effektivisera sina verksamheter genom enkla, automatiska och datorbaserade processer som är lätta att använda för medarbetare och medborgare. I sådana processer är det viktigt att myndigheten aktivt vidtar åtgärder för att skydda den grupp av personer som lever under hot.

[1] Prop. 2017/18:145, Ökat skydd för hotade och förföljda personer samt några åtgärder för att öka kvaliteten i folkbokföringen, s 77 och 88.

Den offentliga förvaltningen ska likabehandla individer. För att uppnå denna likabehandling kan myndigheter behöva erbjuda personer där det finns en hotbild att använda alternativa processer för att inte utsätta dessa personer för risker.

1.1 Syfte

Syftet med denna promemoria är att ge ett praktiskt stöd och konkreta tips vid myndigheters hantering av skyddade personuppgifter. Promemorian är avsedd att komplettera och, i vissa delar, ge en fördjupande beskrivning till *Skatteverkets vägledning för offentliga aktörers hantering av skyddade personuppgifter*.

I promemorian berörs också det vidare perspektivet, att det finns personer med ett skyddsbehov, men som inte har skyddade personuppgifter och därmed inte har samma lagstiftningsmässiga skydd som personer med skyddade personuppgifter.

1.2 Målgrupp

Promemorian är framtagen för eSams medlemmar men bör vara relevant för alla myndigheter och även kommuner, regioner och kommunförbund.

Målgrupp för promemorian är främst medarbetare inom respektive myndighet som ska hantera skyddade personuppgifter. Det kan till exempel handla om handläggare eller medarbetare som ansvarar för att ta fram processer, utveckla och anpassa it-system och har särskilda roller inom exempelvis informationssäkerhet, arkivhantering, juridik och personsäkerhet.

1.3 Avgränsningar

Promemorian omfattar inte Skatteverkets egen hantering i folkbokföringen eller Polisens hantering av fingerade personuppgifter. Promemorian berör inte heller dataskyddsregelverkets bestämmelser om känsliga personuppgifter. Detta regelverk behöver dock beaktas parallellt med bestämmelserna om skyddade personuppgifter.

Promemorian tar i första hand sikte på hantering av skyddade personuppgifter. I viss utsträckning berörs att personer kan ha ett skyddsbehov även om de inte har skyddade personuppgifter, se särskilt avsnitt 4.4.

Många av de personer som har skyddade personuppgifter kan också vara föremål för åtgärder från olika myndigheter såsom insatser från socialtjänst, kontaktförbud för en hotaktör[2] vittnesskydd eller personsäkerhetsskydd från Polisen. Det finns ett stort behov

[2] Begreppet förklaras i avsnitt 2.6.

av att på ett bättre sätt inom den offentliga förvaltningen samordna dessa insatser. Förslag till sådana åtgärder ingår inte i denna promemoria.

1.4 Medverkande

Arbetet har genomförts av en arbetsgrupp bestående av Camilla Karp (Skatteverket), Ulrika Conwaliemark (E-hälsomyndigheten), Feyza Kocak (Skolverket), Susanne Eriksson (Försäkringskassan), Christian Slydal Thomassen (Försäkringskassan), Torbjörn Näslund (Skolverket), Renata Wallin (Domstolsverket), Katarina Larsson (Transportstyrelsen), Julia Paulsson (Stockholms stad), och Linda Lindström (eSams kansli). Kvalitetssäkring har skett i eSams rättsliga expertgrupp, expertgruppen i säkerhet samt koordineringsgruppen för arkitektur. Beredning har skett via eSams samordningsgrupp.

2. Begrepp

I detta avsnitt beskrivs begrepp som används i promemorian. Flera av dessa begrepp finns också mer utförligt beskrivna i *Skatteverkets vägledning för offentliga aktörers hantering av skyddade personuppgifter*.

2.1 Skyddade personuppgifter

Skyddade personuppgifter används ofta som samlingsrubrik för de olika skyddsåtgärderna inom folkbokföringen; fingerade personuppgifter,[3] skyddad folkbokföring och sekretessmarkering. I den här promemorian avser begreppet endast skyddad folkbokföring och sekretessmarkering.

Det är Skatteverket som beslutar om skyddade personuppgifter. För att kunna fatta ett sådant beslut måste personen vara folkbokförd i Sverige och ha ett svenskt personnummer.

2.2 Skyddad folkbokföring

Skyddad folkbokföring kan registreras i folkbokföringsdatabasen av Skatteverket när en person av särskilda skäl kan antas bli utsatt för brott, förföljelser eller allvarliga trakasserier, 16 § folkbokföringslagen (1991:481) (FOL). Sekretessen för uppgifterna i folkbokföringsdatabasen gällande den som har skyddad folkbokföring regleras i 22 kap. 2 § offentlighets- och sekretesslagen (2009:400) (OSL).

2.3 Sekretessmarkering

Skatteverket kan registrera en *sekretessmarkering* i folkbokföringsdatabasen om det finns särskild anledning att anta att en person eller någon närstående till denne riskerar att lida men om uppgifter om personen lämnas ut (22 kap. 1 § OSL). En sekretessmarkering har ingen självständig betydelse utan är en *varningssignal* om behovet av att göra en noggrann skadeprövning enligt tillämplig sekretessbestämmelse.

2.4 Person med skyddsbehov

I promemorian används *person med skyddsbehov* alternativt *skyddsbehövande* för att benämna någon som behöver skyddas på grund av en hotbild. Ibland har en sådan person skyddade personuppgifter, men det kan föreligga ett skyddsbehov även om personen

[3] Fingerade personuppgifter regleras i lagen (1991:483) om fingerade personuppgifter. Fingerade personuppgifter är den högsta nivån av skyddade personuppgifter i Sverige och hanteras av Polismyndigheten. https://polisen.se

inte har skyddade personuppgifter, se avsnitt 4.4. En person med skyddsbehov kan t.ex. vara en patient, elev eller klient. I relationen med myndigheter används ibland begreppet kund eller sökande. Det kan också vara en medarbetare på den egna myndigheten.

2.5 Person med skyddade personuppgifter

Person med skyddade personuppgifter avser i denna promemoria en person som i folkbokföringen antingen har en sekretessmarkering eller skyddad folkbokföring.[4]

2.6 Hotaktör

Begreppet *hotaktör* används i denna promemoria för den eller de personer eller organisationer som utsätter personer för hot. Hotet kan handla om ett direkt fysiskt angrepp, men också om andra typer av angrepp exempelvis digitalt angrepp, psykiskt eller ekonomiskt våld eller förtal. En hotaktör kan vara en extern aktör, men skulle även kunna vara en anställd i en samhällsfunktion, t.ex. en myndighet.

2.7 Person som hanterar skyddade personuppgifter

Med *person som hanterar skyddade personuppgifter* avses medarbetare på en myndighet som hanterar sådan information. Det kan t.ex. vara en handläggare, chef eller annan medarbetare.

2.8 Terminologi som bör undvikas

Begreppet och processen kvarskrivning har ersatts av *skyddad folkbokföring*. Kvarskrivning bör därmed inte längre användas.

Ibland används skyddad identitet (SID) parallellt eller i stället för skyddade personuppgifter. Begreppet har ofta en bredare betydelse och används även vid fingerade uppgifter, varför det finns en risk att blanda ihop vilket skydd som föreligger. Det är bättre att använda begreppet *skyddade personuppgifter* när skyddad folkbokföring och sekretessmarkering åsyftas.

[4] I andra dokument räknas oftast även personer med fingerade personuppgifter med i denna grupp.

3. Rättsliga förutsättningar för skyddade personuppgifter

I detta avsnitt redovisas kort bestämmelserna om folkbokföringssekretess. För en utförligare redogörelse se *Skatteverkets vägledning för offentliga aktörers hantering av skyddade personuppgifter*. I avsnittet berörs dessutom andra sekretessbestämmelser som kan aktualiseras när myndigheten ska pröva om uppgifterna kan skyddas.

3.1 Sekretess vid skyddad folkbokföring

Sekretessen för uppgifterna i folkbokföringsdatabasen för den som har skyddad folkbokföring regleras i 22 kap. 2 § OSL. Denna bestämmelse tillämpas av Skatteverket och innebär att sekretess gäller i ärende om skyddad folkbokföring för uppgift om en enskilds personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Här är presumtionen att uppgifterna omfattas av sekretess.

Får en myndighet uppgifter om en person med skyddad folkbokföring från Skatteverket gäller skyddet i 22 kap. 2 § OSL även hos den mottagande myndigheten enligt 22 kap. 3 § OSL.

Sekretess gäller också, enligt 21 kap. 3 § a första stycket OSL, i mål eller ärende vid domstol eller annan myndighet där en part har skyddad folkbokföring, för uppgift som lämnar upplysning om var den parten bor stadigvarande eller tillfälligt, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men. Detsamma gäller om uppgiften tillsammans med annan uppgift i målet eller ärendet bidrar till sådan upplysning. Även här är presumtionen att uppgifterna omfattas av sekretess. Bestämmelsen är generellt tillämplig i mål och ärenden som gäller all offentlig verksamhet.

3.2 Sekretessmarkering

Inom folkbokföringen gäller även 22 kap. 1 § OSL. Bestämmelsen omfattar enskilds personliga förhållanden om det av särskild anledning kan antas att den enskilde eller närstående lider men om uppgiften röjs, dvs. det gäller en presumtion för offentlighet. Denna sekretess omfattar, förutom folkbokföringsregistret, även vissa andra register (se 6 § offentlighets- och sekretessförordningen). Som exempel på sådana register kan nämnas Polismyndighetens passregister och register över nationella identitetskort,

Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal, samt Transportstyrelsens vägtrafikregister. Om Skatteverket bedömer att uppgifter kan omfattas av sekretess enligt 22 kap. 1 § kan myndigheten besluta om att registrera en sekretessmarkering i folkbokföringsdatabasen.

3.3 Andra sekretessbestämmelser som kan aktualiseras

En myndighet som ska bedöma om de skyddade personuppgifterna omfattas av sekretess behöver dels beakta sekretessbestämmelserna inom folkbokföringen för skyddade personuppgifter (vid fråga om sådana uppgifter), dels beakta andra tillämpliga sekretessbestämmelser. Det är upp till varje myndighet att ta ställning till vilka sekretessbestämmelser som omfattar just dess verksamhet och de uppgifter som den hanterar.

Förutom en prövning enligt 22 kap. 1 § OSL som nämns i stycket ovan och som är tillämplig för vissa myndigheter, har en myndighet att pröva en begäran om uppgifter enligt särskilda sekretessbestämmelser i OSL som gäller den aktuella verksamheten eller specifika uppgifter om en person. Sådana bestämmelser kan därmed också aktualiseras vid hantering av skyddade personuppgifter.

Hos alla myndigheter gäller i vissa fall sekretess för vissa bostads- och kontaktuppgifter om förföljda personer (21 kap. 3 § OSL). Detta är en generell sekretessbestämmelse där det råder en presumtion för att uppgifterna är offentliga. Det ska göras en individuell prövning i varje enskilt fall. Skulle en myndighet få information om att en person eller dess anhörig är förföljd och det av särskild anledning kan antas att de kan komma att utsättas för hot eller våld eller lida annat allvarligt men kan denna paragraf tillämpas. Som exempel på uppgifter som omfattas av särskilda sekretessbestämmelser är uppgifter om personers hälsa eller sexualliv (21 kap. 1 § OSL), uppgifter om personliga enskilda förhållanden i utbildningsverksamhet (23 kap. 1 § OSL) samt uppgifter hos socialtjänsten (26 kap. 1 § OSL).

Även personaladministrativ sekretess kan komma att bli tillämplig (39 kap. OSL).

En myndighet kan sekretessmarkera en uppgift i en allmän handling om uppgiften kan antas omfattas av en sekretessbestämmelse (5 kap. 5 § OSL). Sådan markering görs på handlingen eller i den databas den elektroniska handlingen hanteras.

Samma uppgift om en person kan i vissa fall omfattas av flera sekretessbestämmelser i OSL. Huvudregeln är då att myndigheten ska tillämpa den bestämmelse som ger det starkaste skyddet (7 kap. 3 § OSL).

4. Om skyddsbehov

4.1 Skyddsbehov

Skatteverket beslutar om skyddad folkbokföring och sekretessmarkering i folkbokföringen. Kriterierna för skyddad folkbokföring är att det föreligger ett skyddsbehov på grund av särskild risk att utsättas för brott, förföljelser eller allvarliga trakasserier. För sekretessmarkering gäller att Skatteverket bedömer att det kan finnas särskild anledning att anta att en person eller någon närstående till denne riskerar att lida men om uppgifter om personen lämnas ut. En skadebedömning måste dock göras i det enskilda fallet. För att kunna få skyddad folkbokföring eller sekretessmarkering behöver personen vara folkbokförd i Sverige och ha ett svenskt personnummer. Som tidigare nämnts kan det också förekomma att personer kan ha ett skyddsbehov utan att ha skyddade personuppgifter, se avsnitt 4.4.

Ett skyddsbehov kan föreligga av många olika orsaker. Skyddsbehovet kan exempelvis vara föranlett av direkt hot och våld, men också trakasserier. Ofta kan det vara fråga om en hotbild i en nära relation. Skyddsbehovet kan även gälla anhörig till personen med skyddsbehov, se avsnitt 4.3. Det kan föreligga ett skyddsbehov på grund av hot från kriminella nätverk eller hot mot avhoppare från repressiva regimer. Vissa grupper inom rättsväsendet såsom åklagare eller enskilda polismän kan också behöva skydd. Andra som kan ha ett skyddsbehov är personer som vittnat i en rättegång, personer i konkurrerande kriminella nätverk, etc. Ett skyddsbehov kan även föreligga på grund av könsbyte eller förföljelse.

Det vanligaste skyddsbehovet avser skydd för uppgift som kan bidra till att personen kan lokaliseras; såsom var personen bor, arbetar, studerar eller har inbokade möten, se avsnitt 5 om skyddsvärda uppgifter.

När en myndighet samlar in information om personer med skyddade personuppgifter medföljer ett ansvar att skydda informationen. Myndigheten måste själv bedöma vilken information som behöver skyddas för att tillgodose skyddsbehovet. Förutom uppgifter från folkbokföringen, se avsnitt 6.1 om Navet, kan uppgifter även komma till myndigheten från personen själv, en närstående eller genom att de har samlats in på annat sätt. Det kan också vara information som myndigheten själv har skapat. Myndigheten behöver undersöka vilka uppgifter som finns i de egna systemen och som kan bli skyddsvärda när myndigheten får information om ett skyddsbehov. De skyddsvärda uppgifterna behöver hanteras varsamt. Om uppgifterna röjs ökar risken för

den som har skyddsbehovet. Det är viktigt att de personer på myndigheten som hanterar skyddade personuppgifter har rätt kompetens för uppgiften.

4.2 Hotaktören försöker komma åt uppgifterna

De skyddsbehövande har behov av skydd på grund av att en eller flera hotaktörer försöker hitta dem. Många hotaktörer lägger ner avsevärda resurser på att spåra den de vill komma åt. Exempel på hur hotaktören kan försöka komma åt de skyddade uppgifterna är:

- Att någon ringer och falskt utger sig för att vara den skyddsbehövande.
- Att någon ringer och påstår att den skyddsbehövande behöver hjälp och att det är viktigt att snabbt få kontakt med hen, t.ex. för att den skyddsbehövande påstås vara utsatt för livsfara.
- Att någon ringer och falskt utger sig för att arbeta på socialtjänsten, Polisen, Skatteverket, eller någon annan myndighet och som vill diskutera skyddet. Den som ringer kan också påstå sig företräda en organisation, t.ex. ett kvinnohus.

En hotaktör kan ha en väl uppbyggd historia och kan successivt ha samlat ihop information från olika aktörer. Det kan därför vara svårt att upptäcka att det är fråga om en hotaktör. Anställda på myndigheter har en serviceskyldighet och ska vara hjälpsamma och tillmötesgående. I ärenden som kan innehålla skyddade personuppgifter är det emellertid väldigt viktigt att vara vaksam mot obehöriga som försöker komma åt information som de inte ska ha. Om skyddade personuppgifter röjs kan det innebära fara för den skyddsbehövande. Risken för bedrägliga försök att komma åt informationen är ett av skälen till att det ofta behövs särskilda handläggare för att hantera skyddade personuppgifter, se vidare i avsnitt 8.2. Se även avsnitt 8.3 om motringning.

Andra exempel på hur en hotaktör kan försöka få ut uppgifter om en skyddsbehövande är:

- Att begära ut allmänna handlingar som kan indikera var den skyddsbehövande bor eller befinner sig.
- It-intrång av olika slag för att komma åt uppgifter om den skyddsbehövande.
- Infiltration i en myndighet.

Hotaktörer kan lägga stora resurser på att komma åt information. Om de ingår i kriminella nätverk kan det finnas ett stort kapital att tillgå. Hotaktörer kan köpa information från personer som är beredda att sälja, utöva utpressning eller hota personer som man tror skulle kunna skaffa sig information, till exempel i tjänsten.

Är hotaktören en främmande makt finns sannolikt avsevärda resurser både i kapital och tid för it-intrång, hot och utpressning, psykologiska drivkrafter, osv.

Ovanstående ska ses som exempel på bredden av hotaktörer och åtgärder som kan användas för att komma åt uppgifter om en skyddsbehövande.

4.3 Hela familjen omfattas av skyddsåtgärderna

Eftersom skyddsbehovet ofta handlar om ett behov av att skydda uppgifter om var den skyddsbehövande vistas, så måste samma skyddsåtgärder (skyddad folkbokföring eller sekretessmarkering i folkbokföringen) vanligtvis omfatta samtliga som bor tillsammans.

En relativt stor del av personer med skyddade personuppgifter är barn. Det föreligger en särskild risk för att en hotaktör får tillgång till uppgifter om plats eftersom barn inte förstår risken och gärna vill vara med på klassfoton och andra event tillsammans med sina klasskamrater eller vänner. Det vara svårt att veta vilka vuxna som kan informeras om hotbilden. Det är också en svår avvägning om man ska berätta för ett barn att det finns ett skyddsbehov.

Det finns luckor i skyddet för närstående. Ett exempel är om en folkbokförd person A som har en hotbild bor tillsammans med person B som har samordningsnummer. En person med samordningsnummer, som ännu inte är folkbokförd, kan inte få skyddade personuppgifter, se avsnitt 4.4. Det innebär att person A kan ha skyddad folkbokföring men inte person B. Eftersom person B har ett samordningsnummer, så saknar de flesta myndigheter kännedom om att även person B:s uppgifter behöver skyddas för att upprätthålla skyddet för person A. Om sammanboendet är känt för hotaktören, kan det innebära att skyddsåtgärden gentemot person A därmed tappar all verkan.

Ett annat exempel är ett barn boende hos sin mamma som har skyddade personuppgifter. Även barnet har då skyddade personuppgifter. Pappan kan vara hotaktören, men kan samtidigt ha umgängesrätt med barnet. Även om socialtjänsterna försöker hitta lösningar för detta, så får man ha i åtanke att pappan kan försöka få fram uppgifter om mammans och barnets boende på sätt som barn inte kan inse eller där barnet hamnar i en lojalitetskonflikt.

Det kan vara utmanande för myndigheter att hantera situationer som beskrivs i exemplen. Därför är det särskilt viktigt att de personer som hanterar uppgifterna har rätt kompetens.

4.4 Personer som har skyddsbehov men som inte omfattas av skyddsåtgärderna i folkbokföringen

Endast personer som är folkbokförda i Sverige vid ansökningstillfället kan få skyddade personuppgifter. Bor man utomlands eller har samordningsnummer är man inte folkbokförd i Sverige och kan därmed inte få skyddade personuppgifter. Detsamma gäller personer som saknar såväl personnummer som samordningsnummer.

Även om dessa personer inte omfattas av skyddet i folkbokföringen behöver en myndighet vara medveten om att det kan finnas behov av att vissa personer inom nämnda personkategorier skyddas i den offentliga förvaltningen, se avsnitt 3 om bland annat sekretess enligt 21 kap. 3 § OSL.

5. Skyddsvärda uppgifter

Vilka uppgifter som behöver skyddas kan variera beroende på personens skyddsbehov. I detta avsnitt redogörs för uppgifter som typiskt sett kan behöva skyddas. Observera att listan inte är uttömmande och att även andra uppgifter kan vara skyddsvärda. För att skydda en uppgift behöver det finnas en tillämplig sekretessbestämmelse. Det behöver således alltid undersökas vilka tillämpliga sekretessbestämmelser som föreligger för en viss uppgift. Många sekretessbestämmelser innebär att det ska göras en skadeprövning för att bedöma om sekretess föreligger i det enskilda fallet.

Även information som gällde innan personen fick ett skyddsbehov kan behöva skyddas. Detta eftersom den skyddsbehövande kanske fortsätter att arbeta hos samma arbetsgivare, besöka samma läkarmottagningar, ha samma handläggare för sina ärenden, etc.

5.1 Geografisk information

Geografiska uppgifter kopplade till den skyddsbehövande är i princip alltid skyddsvärda uppgifter. Det avser t.ex. uppgifter om var den skyddsbehövande bor, arbetar och var barnen går i skola. Det kan också handla om vilka kontor eller mottagningar som har besökts, vilka arbetsgivare som personen har sökt arbete hos och så vidare, det vill säga information som bidrar till att identifiera var den skyddsbehövande befinner sig vid olika tillfällen.

Telefonnummer är ofta skyddsvärda av flera olika skäl. Geografiska riktnummer kan peka på var personen befinner sig och telefonnummer kan användas i bedrägliga försök eller för att trakassera den skyddsbehövande både psykiskt och ekonomiskt.

5.2 Indirekt geografisk information

Det finns även uppgifter som indirekt kan ge en hotaktör tillgång till geografiska uppgifter. Exempelvis kan ett namn på eller en signatur av en handläggare användas för att få en uppfattning om vilket kontor den skyddsbehövande har besökt. Detsamma gäller t.ex. telefonnummer, e-postadress eller andra uppgifter till en handläggare.

Beslutsnummer, diarienummer, kundnummer, etc. skulle också kunna användas av en hotaktör i avsikt att få fram information om den skyddsbehövande. Även namn på juridiskt ombud eller annat ombud, namn på en närstående, eller liknande, kan användas av hotaktören i försöken att lokalisera den skyddsbehövande.

5.3 Personnummer

Personnumret är ofta den enda uppgift som myndigheten kan hantera öppet för personer med skyddade personuppgifter, se avsnitt 7.6. Ett personnummer utan koppling till andra uppgifter är i sig sällan skyddsvärt, men problemet är att personnumret ofta förekommer i ett sammanhang, och detta sammanhang kan göra uppgiften skyddsvärd.

Om personnumret t.ex. används i en anmälningslista till ett digitalt seminarium bör skyddsvärdet inte vara högt. Om det däremot framgår i anmälningslistan att seminariet kommer att äga rum på platsen A blir uppgiften betydligt mer skyddsvärd, eftersom kombinationen kan innebära ett röjande av var personen befinner sig vid en viss tidpunkt.

5.4 Namn

Uppgift om namn kan ha en koppling till geografiska uppgifter och därmed vara skyddsvärt. Uppgift om namn kan dessutom röja att den skyddsbehövande har ändrat sitt namn som en del i att skapa ett skydd, om en koppling finns mellan dessa namn. Utan att ha fått mer detaljerade uppgifter om den skyddsbehövandens hotbild, bör myndigheten anta att personens namn har ett högt skyddsvärde. Det bör noteras att namn inte omfattas av sekretessbestämmelsen i 21 kap. 3 § OSL, vilket innebär att en uppgift om namn inte kan skyddas enligt den bestämmelsen.

6. Skatteverkets service kring personer med skyddade personuppgifter

6.1 Navet

Via Skatteverkets tjänst Navet kan myndigheter få information om vilka personer som har skyddad folkbokföring eller en sekretessmarkering. Via Navet kan myndigheten också få information om förändringar, dvs. om en person fått skyddad folkbokföring istället för sekretessmarkering eller tvärtom, eller om skyddet har tagits bort. Skatteverket kan inte lämna ytterligare information till myndigheten eller dess medarbetare om vari hotbilden eller skyddsbehovet består.

Myndigheten kan prenumerera på tjänsten och få dagliga uppdateringar. I Navet visas uppgift om sekretessmarkering med en flagga och skyddad folkbokföring med två flaggor. Information kan också erhållas genom en automatiserad slagning eller en manuell slagning i samband med att ett utlämnande ska prövas. Myndighetens behov av att ta del av information om skyddsnivå behöver övervägas noggrant. Vid anslutning till Navet behöver myndigheten välja vilka uppgifter man tar emot utifrån vilka uppgifter man kan skydda.

6.2 Postförmedlingstjänster

Skatteverket tillhandahåller postförmedlingstjänster dit brev, rekommenderat brev och paket kan skickas. Posten skickas till en boxadress till ett skattekontor, som förmedlar posten till personerna med skyddade personuppgifter. Det brev som ska förmedlas ska läggas i ett kuvert, kuvertet ska klistras igen och på kuvertet ska anges fullständigt personnummer. På baksidan ska avsändaradress anges. Det igenklistrade kuvertet ska därefter läggas i ett ytterkuvert som adresseras till någon av Skatteverkets boxadresser.

Postförmedlingstjänsterna finns på skattekontor på flera orter och med olika boxadresser, se Skatteverkets webbplats.

6.3 Upplysningtjänst

Skatteverket lämnar också information om att en person med ett visst personnummer har skyddade personuppgifter, se kontaktinformation på Skatteverkets webbplats. En person som ringer Skatteverkets upplysningstjänst och anger personnummer på en person, kan få svaret att personen har skyddade personuppgifter. Ytterligare information kommer inte att lämnas.

7. Exempel på missuppfattningar och utmaningar

I detta avsnitt beskrivs missuppfattningar eller utmaningar som kan förekomma hos myndigheter.

7.1 Fler uppgifter är skyddsvärda

En missuppfattning hos vissa myndigheter är att det endast är de uppgifter som hämtas från Navet som myndigheten ska skydda. Skyddsvärda uppgifter kan dock komma från den person som skyddet gäller, en närstående eller vara uppgifter som myndigheten samlat in från andra källor. Har myndigheten fått kännedom om att en person har ett skyddsbehov finns ofta ett behov att skydda stora mängder information om personen och dennes kontakter med myndigheten för att åstadkomma ett adekvat skydd. Detta beror på att befintliga eller tillkommande uppgifter på myndigheten kan användas för att indikera var personen med skyddsbehov befinner sig. Uppgifter som kan behöva skyddas är exempelvis uppgifter om skola och handläggande ort. Myndigheten behöver undersöka vilka uppgifter som behöver skyddas utifrån tillämpliga sekretessbestämmelser.

7.2 Även äldre uppgifter kan behöva skyddas

Det är en missuppfattning att skyddet endast gäller den information som kommer in eller som upprättas efter det att personen fått skyddade personuppgifter. Personens skyddsbehov innebär dock att mängder av uppgifter som är direkt eller indirekt kopplade till personen med skyddsbehov behöver skyddas. Detta gäller även uppgifter som tillkommit före det att personen fått skyddade personuppgifter. Det kan till exempel röra namnbyte eller könsbyte då det gamla namnet respektive det gamla personnumret också behöver skyddas.

7.3 Navet ger inte alltid en fullständig information

Det är en missuppfattning att den information som hämtas från Navet ger en fullständig information om skyddsbehov. En person kan ha ett skyddsbehov och hotbild utan att ha skyddade personuppgifter, se avsnitt 4.4.

Myndigheter har alltid en skyldighet att skydda sekretessbelagda uppgifter och se till att uppgifterna inte röjs för obehöriga, oavsett om det finns en sekretessmarkering eller inte.

7.4 Hotaktören kan finnas var som helst

En missuppfattning är att hotaktören finns utanför den egna myndigheten eller utanför den offentliga förvaltningen. Myndigheten måste emellertid utgå från att hotaktören kan finnas var som helst, inklusive i den egna verksamheten.

7.5 Det kan finnas behov av anpassade rutiner

Det kan vara en missuppfattning att generella rutiner alltid är tillräckliga. Myndigheten behöver ha rutiner som fungerar väl för alla personer med skyddsbehov och för de som ska tillämpa dem. Det behöver dock finnas en förståelse i organisationen för att personer som arbetar med dessa uppgifter i vissa fall kan behöva anpassa tillämpningen utifrån den specifika situationen.

7.6 Personnummer har inte alltid ett högt skyddsvärde

En missuppfattning kan vara att myndigheter antar att personnummer på personer med skyddade personuppgifter alltid har ett högt skyddsvärde. Detta leder ofta till problem på myndigheterna. Personnumret är ofta den enda uppgift som myndigheten kan hantera öppet för personer med skyddade personuppgifter. Det innebär att det ofta kan vara så att myndigheten anger personnummer i kommunikation och beslut när det annars t.ex. skulle anges namn och adress. Myndigheten identifierar individen med personnummer i beslutsfattandet och myndigheten ska utelämna skyddsvärda uppgifter som namn och adress när stöd finns i sekretessbestämmelserna.

Ibland har dock personnumret högt skyddsvärde om det förekommer i sammanhang som t.ex. innebär en koppling till geografisk information. Det är en utmaning för myndigheter att utbilda och förklara för de personer som hanterar skyddade personuppgifter när personnummer till personer med skyddade personuppgifter är skyddsvärda och när de inte är det.

7.7 Egna identifikationsnummer kan ge falsk trygghet

I vissa fall förekommer s.k. reservnummer eller andra fiktiva nummer eller koder istället för ett personnummer som identifikation. Personen med skyddsbehov kan missuppfatta att användningen av ett sådant nummer eller kod ger samma skydd som att ha skyddade personuppgifter och personen invaggas därmed i en falsk trygghet. Det kan till exempel också innebära att man inte kan hämta eller får rätt uppgifter från Navet. Om möjligt bör myndigheter undvika att använda egna nummerserier eller koder.

7.8 Bedömning av utlämnandet behöver alltid göras

Ett missförstånd är att om skyddade personuppgifter kan lämnas över mellan två myndigheter utifrån en sekretessbrytande regel så omfattas de inte av sekretess. Det stämmer inte. Sekretessen gäller alltjämt för uppgifterna hos den första myndigheten. Sekretessen kan vidare föras över så att den gäller även hos den andra myndigheten. Dessutom kan uppgifterna träffas av ytterligare sekretessbestämmelser som gäller för den mottagande myndighetens verksamhet.

Sekretessbrytande regler syftar ofta till att sakförhållanden kring olika personer ska kunna utbytas mellan myndigheter, trots att de annars omfattas av sekretess. Behovet är i allmänhet väl utrett och motiverat. Ibland kan det ändå finnas svårigheter med att skydda en uppgift som har förts över från en annan myndighet, beroende på vilka sekretessbestämmelser som blir tillämpliga. Då kan det t.ex. finnas skäl att fundera på om man ska begära in uppgiften från den andra myndigheten. Både avsändande och mottagande myndighet behöver alltid överväga uppgiftsminimering, dvs. bedöma vilka uppgifter som det är nödvändigt att ta del av.

Myndigheten behöver alltid göra en egen bedömning av om uppgifter kan lämnas ut eller inte. På vilket sätt och till vem ett utlämnande sker hos den mottagande myndigheten bör ske enligt fastställda rutiner, se avsnitt 8.3.

7.9 Motringning är inte alltid en effektiv metod

Många myndigheter rekommenderar att man aldrig ska lämna ut skyddsvärd information i ett telefonsamtal vid hantering av personer med hotbild. Rekommendationen är att motringa till den andra personen innan man lämnar ut uppgifterna. Ofta finns det inga andra metoder att ta till.

Personen som hanterar skyddade personuppgifter på myndigheten behöver dock vara uppmärksam på att inte luras in i en falsk trygghet. Det är att föredra att motringa via växelnummer eller helst att det finns en förutbestämd process om hur utlämnande av uppgift ska ske, se avsnitt 8.3 om råd kring motringning.

8. Tips vid hantering

Detta avsnitt är avsett att komplettera Skatteverkets vägledning och avsnittet följer dispositionen i vägledningen för att underlätta vid samläsning av de båda dokumenten.

8.1 Riskminimering vid hantering av skyddade personuppgifter

8.1.1 Analys av myndighetens skyddsvärda uppgifter och hantering i myndighetens it-system

1. Har myndigheten analyserat vilka uppgifter som behöver skyddas?

Att tänka på: Myndigheten behöver analysera de informationsmängder som hanteras i myndighetens it-system för att bedöma om det är skyddsvärda uppgifter. Skyddade personuppgifter kan komma till myndigheten på olika sätt. Olika typer av uppgifter kan behöva skyddas. Även uppgifter som tillkommit före det att personen fått skyddade personuppgifter kan behöva skyddas. Myndigheten behöver också analysera tillämpliga sekretessbestämmelser för de skyddsvärda uppgifterna.

2. Har myndigheten övervägt vilka uppgifter som ska hämtas från Navet utifrån myndighetens förutsättningar att skydda dessa uppgifter?

Att tänka på: Myndigheten bör analysera vilka olika avtal som finns för kanaler att hämta information ur Navet. Behövs alla kanalerna eller kan de begränsas? Följer Navets flaggor med vid hämtningen av uppgifterna? Myndigheten bör analysera om hämtningen ska ske automatiserat eller manuellt och hur ofta hämtning ska ske. Myndigheten bör inte hämta mer uppgifter än vad som behövs.

3. Har myndigheten analyserat i vilka av myndighetens system som skyddade personuppgifter hanteras?

Att tänka på: I vissa fall sparas uppgifter i teknisk utrustning såsom skrivare, usb och datorer och myndigheten behöver säkerställa att sådan information raderas. I vissa fall kan det finnas skäl att begränsa vilka skrivare som får användas för utskrift av skyddade personuppgifter. Om möjligt bör myndigheten undvika att göra egna markeringar (såsom en egen flagga utöver de flaggor som kommer med Navet) eller egna anteckningar som kan vara svåra att hålla reda på.

4. Hur har myndigheten säkerställt att information om en skyddad personuppgift når alla system där uppgiften finns?

Att tänka på: Det är att föredra att hanteringen är inbyggd i systemet. Om detta inte är möjligt behöver myndigheten säkerställa att det finns rutiner för manuell hantering. Om en handläggare t.ex. gör en manuell slagning i Navet behöver handläggaren veta vilka åtgärder hen förväntas vidta för att informationen ska nå övriga verksamheten och dess system. Myndigheten behöver också säkerställa en fortsatt uppdatering. Detsamma gäller om en person själv lämnar sådan uppgift t.ex. i samband med ett ärende.

5. Har myndigheten säkerställt att obehöriga inte kan ta del av de skyddade personuppgifterna?

Att tänka på: En stark rekommendation är att systemen har en behörighetsstyrning så att åtkomsten kan begränsas till de som ska kunna se skyddade personuppgifter. Åtkomstkontroll bör genomföras. Myndigheten behöver bestämma vilka anställda som ska kunna se vad. Myndigheterna bör också fundera över utformningen av felmeddelandetexter så att det, när det bedöms vara befogat, framgår att åtkomsten är begränsad för att det är fråga om en skyddad personuppgift så att inte it-support får felanmälningar i onödan. Det bör, om möjligt, finnas larmfunktioner som kan upptäcka eventuella incidenter gällande skyddade personuppgifter i it-systemen.

8.2 Särskild behörighet

8.2.1 Vilka på myndigheten ska hantera dessa ärenden?

6. Har myndigheten bestämt vilka på myndigheten som ska hantera ärenden där personen har skyddade personuppgifter?

Att tänka på: Att hantera ärenden med skyddade personuppgifter är komplext och en felaktig hantering kan få allvarliga konsekvenser för den skyddsbehövande. Om en myndighet har verksamhet på flera orter kan myndigheten eventuellt överväga att koncentrera hanteringen av skyddade personuppgifter till en ort för att undvika att skicka uppgifter. Samtidigt kan det finnas en risk om det kommer fram att alla dessa uppgifter hanteras på ett specifikt kontor. Ett alternativ är att utse en särskild grupp som inte sitter tillsammans geografiskt. Myndigheten behöver då säkerställa att det finns säkra kommunikationsvägar för den gruppen. Ibland räcker det inte med en grupp, det kan t.ex. finnas behov av en separat grupp som hanterar medarbetare med skyddsbehov skilt från övrig hantering av personer med skyddsbehov. Det är inte heller alltid möjligt att ha särskilda grupper. Lärare behöver t.ex. kunna hantera sådana uppgifter i sin egen klass. Hos vissa regioner finns en grupp som hanterar ärenden där det förekommer skyddade personuppgifter och t.ex. upplyser en läkare innan ett läkarbesök om att det är fråga om en person med skyddsbehov som behöver hanteras på ett visst sätt.

Om extern hantering förekommer, t.ex. av konsulter eller vid utkontraktering, behöver myndigheten överväga hur denna hantering ska utformas.

8.2.2 Kunskap och kompetens

7. Har myndigheten säkerställt att personalen har kunskap om hantering av skyddade personuppgifter?

Att tänka på: Samtliga personer inom myndigheten som kan komma i kontakt med skyddade personuppgifter behöver ha tillräcklig kompetens att hantera informationen i utförandet av sina arbetsuppgifter. Det gäller alla medarbetare såsom handläggare, it-personal, personer som arbetar med informationsförvaltning, kommunikatörer och konsulter. Det är att föredra om myndigheten tillhandahåller en obligatorisk utbildning för alla anställda för att uppnå en sådan kompetens.

Medarbetare som hanterar ärenden med personer med skyddade personuppgifter behöver vara betrodda och ha en förmåga att förstå när hotaktörer försöker komma åt information. Medarbetaren behöver vara väl införstådd i ordinarie processer och i vissa fall också ha mandat att anpassa tillämpningen av processerna i det enskilda fallet där det är nödvändigt för att upprätthålla skyddet för den skyddsbehövande. De som har tillgång till skyddade personuppgifter behöver ha integritet och vara svåra att påverka. Det kan därför vara bra att göra en prövning av lämpligheten för de medarbetarna. Ytterligare ett skäl för att göra en sådan prövning är att säkerställa att en anställd som ska ha tillgång till skyddade personuppgifter inte själv har en bakgrund som hotaktör.

8.3 Kommunikation med och om personer med skyddade personuppgifter

8. Har myndigheten rutiner för att kommunicera med och om en person med skyddade personuppgifter?

Att tänka på: Myndigheten behöver alltid överväga vilka kommunikationskanaler som är säkra. Myndigheten bör alltid eftersträva att tillhandahålla e-tjänster där skyddade personuppgifter kan hanteras. Detta bör finnas med i kravställning inför upphandling eller egenutveckling. Om uppgifter om skyddade personuppgifter kan inhämtas direkt och hanteras i enlighet med relevanta processer minskar risken för informationsläckage.

Det är emellertid inte alltid möjligt eller lämpligt att personer med skyddade personuppgifter använder myndighetens e-tjänster, t.ex. att lämna personuppgifter vid ansökan till en tjänst i ett e-formulär. Ett tips är att utforma e-tjänsterna så att det finns en informationstext initialt i e-tjänsten, t.ex. med en hänvisning att personen istället kan

kontakta en specifik handläggare. Personer med skyddade personuppgifter kan uppleva en trygghet i kontakten med en myndighet och lämna mer information än vad som behövs. Myndigheten behöver ha rutiner så man undviker att be om eller registrera fler uppgifter än nödvändigt. Detsamma gäller utformning av beslut. Vid rapportskrivning eller liknande bör avidentifiering göras i den mån det är möjligt.[5] Myndigheten bör ha i åtanke att det kan bli fråga om uppgifter eller handlingar som kan komma att begäras ut.

9. Har myndigheten rutiner för att kommunicera med en annan myndighet om personer med skyddade personuppgifter?

Att tänka på: Vid kommunikation med en annan myndighet bör det finnas fastlagda rutiner, detta minskar risken för att en hotaktör lurar till sig information. Motringning bör ske via växelnummer som hämtats från oberoende källa. Om möjligt bör det finnas särskilda rutiner för överlämning av skyddade personuppgifter till annan myndighet, så att överlämning alltid sker på samma sätt. Det kan vara bra att låta all kommunikation gå via vissa utsedda kontaktpersoner. Det kan finnas skäl till en dialog mellan myndigheterna i syfte att bedöma vilken information det finns behov att ta del av, så att man undviker att lämna över mer uppgifter än vad som är nödvändigt för att mottagande myndighet ska kunna utföra sitt uppdrag.

8.4 Efterlevnad av regler och rutiner

10. Har myndigheten en kontinuerlig uppföljning av hantering av skyddade personuppgifter?

Att tänka på: Myndigheten behöver bestämma vilken loggningsfunktionalitet som ska finnas i systemen för skyddade personuppgifter. Myndigheten behöver också bestämma på vilket sätt dessa loggar ska granskas. Myndigheten bör också ha rutiner för hantering av skyddade personuppgifter i handläggningen och en plan för hur dessa rutiner följs upp. Det kan t.ex. avse begäran om utlämnande och hur skyddsbehovet beaktas i sådana ärenden.

8.5 Om uppgifter röjs

11. Har myndigheten rutiner för hantering vid en incident rörande skyddade personuppgifter?

Att tänka på: Myndighetens rutiner för hantering vid en incident rörande skyddade personuppgifter behöver vara kända inom verksamheten. Det är viktigt att myndigheten

[5] Se t.ex. ES-2022-1 Vägledning Pseudonymisering av personuppgifter om rättsliga förutsättningar.

har dialog med Skatteverket när det inträffat en incident som kan medföra allvarliga konsekvenser för personer med skyddade personuppgifter.

8.6 Skicka post till någon med skyddade personuppgifter

12. Har myndigheten rutiner för hur post skickas till personer med skyddade personuppgifter?

Att tänka på: För att kunna skicka post till personer med skyddade personuppgifter tillhandahåller Skatteverket en förmedlingstjänst, se avsnitt 6.2. Myndigheter kan använda tjänsten för att skicka post till personer med skyddade personuppgifter i de fall de inte har tillgång till personens adressuppgifter. Användning av tjänsten kan innebära att det tar några dagar extra för posten att nå mottagaren.

Om myndigheten har tillgång till sökandes adressuppgifter via Navet kan myndigheten skicka brev till den adressen. Det är dock mycket viktigt att myndigheten är uppmärksam på om personen har en *särskild postadress*, dvs. en annan adress än folkbokföringsadressen (t.ex. en boxadress). Om särskild postadress finns ska posten skickas dit, eftersom folkbokföringsadressen inte alltid är säker att skicka till.

Om personen har tillgång till en digital brevlåda (t.ex. Kivra) kan myndigheten med fördel skicka brev till den istället för att skicka vanlig post, då det är en säker kommunikationskanal. E-post (okrypterad) är som huvudregel inte är en säker kommunikationskanal.

eSam är ett medlemsdrivet program för samverkan mellan myndigheter för att underlätta och påskynda digitaliseringen inom det offentliga. eSam bildades 2015 som en frivillig fortsättning på E-delegationen. En viktig uppgift för eSam är att ta fram stöd och vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Arbetsmiljöverket, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, E-hälsomyndigheten, Ekonomistyrningsverket, Finansinspektionen, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kemikalieinspektionen, Kriminalvården, Kronofogdemyndigheten, Kustbevakningen, Lantmäteriet, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Patent- och Registreringsverket, Pensionsmyndigheten, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet (okt 2023).