Hantering av personer med skyddade personuppgifter

RIKTLINJER

Örebro kommun **2017-12-19** **Ks 1160/2017**
orebro.se

ÖREBRO

PROGRAM
Uttrycker värdegrund och önskvärd utveckling av verksamheten.

POLICY
Uttrycker ett värdegrundsbaserat förhållningssätt och principer för vägledning.

STRATEGI
Konkretiserar ett program eller en policy och utgör en grund för Prioritering.

HANDLINGSPLAN
Beskriver konkreta mål och åtgärder.

RIKTLINJER
Säkerställer ett riktigt agerande och en god kvalitet vid handläggning och utförande.

Beslutad av Anne Andersson, Kommundirektör, den 19 december 2017.

Dokumentansvarig på politisk nivå: Kommunstyrelsen
Dokumentansvarig på tjänstemannanivå: Kommunstyrelseförvaltningen

Sammanfattning

Uppgifter som finns i folkbokföringen är som huvudregel offentliga. En person som är under hot eller förföljelse kan få skyddade personuppgifter. Sekretessmarkering och kvarskrivning beslutas av Skatteverket och att få helt ny identitet, så kallade fingerade personuppgifter, beslutas av Polismyndigheten.

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

Enligt Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter i offentlig förvaltning har den enskilde ett ansvar att själv upplysa om eventuell sekretessmarkering eftersom det inte åligger en myndighet att utan anledning kontrollera om en person har sekretessmarkering i folkbokföringen. I vissa fall hämtar myndigheten uppgifter från folkbokföringen och Skatteverket när personen tar kontakt med myndigheten, i vilka det kan framgå om sekretessmarkering finns.

När en person med skyddade personuppgifter kommer i kontakt med en myndighet som ska registrera, dokumentera och kommunicera gällande den personen behövs tydliga rutiner. Myndigheten ska utreda vad det är som behöver skyddas och varför, för att kunna göra åtgärder för att personen skydd ska bevaras. Genom att begränsa antalet personer som har tillgång till uppgifterna, använda säkra kommunikationskanaler och förvara och hantera uppgifterna på rätt sätt ska säkerheten för den enskilde säkras.

I denna riktlinje beskrivs de olika typerna av skyddade personuppgifter och hur personuppgifterna ska hanteras. Lokala rutiner ska sedan finnas för att beskriva vilka åtgärder som krävs för att säkerställa personens säkerhet och hur denna riktlinje ska efterföljs.

Dataskyddsombud

Den 25 maj 2018 träder dataskyddsförordningen (GDPR) ikraft och ersätter därmed personuppgiftslagen (1998:204). Enligt dataskyddsförordningen ska varje personuppgiftsansvarig (respektive nämnd) utnämna ett dataskyddsombud. Dataskyddsombudet ersätter personuppgiftsombudens roller. Alla frågor som rör skyddet av personuppgifter måste gå via dataskyddsombudet. Bestämmelserna om dataskyddsombud återfinns i artikel 37-39 dataskyddsförordningen.

Innehåll

Inledning

Uppgifter som finns i folkbokföringen är som huvudregel offentliga. I vissa fall kan det dock skada en person om uppgifter om denne lämnas ut. Det kan till exempel gälla någon som är hotad eller förföljd.

”Skyddade personuppgifter” är Skatteverkets samlingsrubrik för de olika skyddsåtgärderna sekretessmarkering, kvarskrivning och fingerade personuppgifter inom folkbokföringen. Alla tre nivåer av skyddade personuppgifter kan kombineras med t.ex. namnbyte.

Sekretessmarkering

Sekretessmarkering innebär att uppgifter om personen enligt folkbokföringens bedömning inte bör lämnas ut utan en särskild sekretessprövning. Detta är den vanligaste formen för skyddade personuppgifter. Om sekretessmarkering anses nödvändig så markerar Skatteverket detta i folkbokföringsdatabasen för den personen. Varje myndighet ska noga sekretesspröva det enskilda fallet innan de lämnar ut uppgifter när någon begär det. Det är alltså ingen absolut sekretess. Mottagande myndighet väljer själv hur den ska hantera sekretessmarkerade uppgifter i sina system. Det framgår inte av själva sekretessmarkeringen vilken personuppgift som är skyddsvärd.

För personer med sekretessmarkering är risken för att skyddade uppgifter av misstag lämnas ut p.g.a. bristande rutiner hos någon myndighet eller organisation ett allvarligt problem. Ofta är det uppgift om vistelse som är extra skyddsvärd. Därför kan det antas att även närstående personer på samma adress skyddas.

Kvarskrivning

Kvarskrivning innebär att en persons verkliga bostadsort och adress hålls hemlig. En person med kvarskrivning är efter flyttning skriven på församlingen på den gamla folkbokföringsorten och med adress hos Skatteverket. Kvarskrivning beviljas endast om behovet av skydd inte kan tillgodoses genom besöksförbud eller på annat sätt. Kvarskrivning kombineras ofta med sekretessmarkering.

För personer med kvarskrivning kan det innebära ett problem att få samhällelig hjälp och service som är knuten till var man är folkbokförd. Den fördröjning som uppstår genom eftersändningen av posten ger ofta upphov till praktiska problem och kostnader.

En person med kvarskrivning ska ha samma rättigheter till handläggning som andra personer. Det är således inte tillåtet att handläggningen försenas för att kommuner inte kan komma överens om vem som ska ge bistånd när personen är skriven och vistas på lika orter eller flyttar ofta. Om det inte finns en stadigvarande vistelsekommun räknas den kommun som personen tillfälligt uppehåller sig i som hemkommun.

Fingerade personuppgifter

Fingerade personuppgifter innebär att en person får byta identitet genom att använda andra personuppgifter än de verkliga. Kopplingen mellan den gamla och den nya identiteten finns endast hos Polismyndigheten. De som kommer ifråga för fingerade personuppgifter är personer som utsätts för särskilt allvarliga hot om liv, hälsa och frihet. Dessa personer behöver bryta helt med sitt tidigare liv inklusive släkt och vänner. Deras omfattande behov av stöd och hjälp tillgodoses till stor del av polisen. Om de behöver stöd genom kommunal service är det ofta polisen som först tar kontakt.

	Sekretessmarkering	Kvarskrivning	Fingerade uppg.
Gäller	En eller flera personuppgifter	Uppgift om var personen befinner sig (ort och adress)	Personens alla personuppgifter
Innebär	En utredning ska göras om vilka uppgifter som är skyddsvärda. Samt en noggrann sekretess-bedömning vid hantering.	Personen skrivs ej på ny adress utan står kvar på sin gamla församling. Skatteverket förmedlar posten.	Helt ny identitet, koppling finns endast hos Polis-myndigheten.
Meddelas	Skatteverket gör en sekretessmarkering i folkbokföringsdatabasen. Den enskilda har också ett ansvar att informera.	Som regel får en kvarskriven person också en sekretessmarkering av Skatteverket.	Den nya identiteten skrivs så att det inte framgår att det rör sig om fingerade personuppgifter.
Enskilda ansöker om detta hos	Skatteverket	Skatteverket	Polismyndigheten
Giltighetstid	Oftast ett år, kan förlängas	Högts tre år i taget.	

Syfte

Riktlinjens syfte är att säkerställa att skyddade personuppgifter hanteras på rätt sätt.

Omfattning

Riktlinjen ska tillämpas av alla nämnder och förvaltningar i Örebro kommun.

Ansvar

Respektive nämnd är en myndighet. Myndigheten ansvarar för att hantera personuppgifter på ett korrekt sätt. Riktlinjen ska göras känd inom myndigheten via de ansvariga tjänstepersonerna. De ska se till att riktlinjen görs känd, att nyanställd personal informeras samt att följa upp hanteringen av skyddade personuppgifter.

Myndigheten ansvarar för att kartlägga behov av lokala rutiner. Varje myndighet ansvarar för att lokala rutiner för hantering av personuppgifter säkerställer att denna riktlinje följs. En rutin ska innehålla sammanställning av åtgärder som ska vidtas när en person med skyddade personuppgifter hanteras.

Giltighetstid

Riktlinjen gäller tillsvidare.

Hantering av personer med skyddade personuppgifter

Myndigheten är personuppgiftsansvarig och måste vidta lämpliga tekniska och organisatoriska åtgärder för att hantera alla personuppgifter som behandlas i organisationen. En säker hantering av skyddade personuppgifter bygger på säkra IT-system och begränsad tillgång till skyddade personuppgifter. Det ska också finnas tydliga rutiner för hur personalen ska hantera skyddade personuppgifter.

Varje myndighet inom Örebro kommun ska utse en särskild person med ansvar för att rutiner och regler för hantering av sekretessmarkerade personuppgifter efterföljs.

Enligt likabehandlingsprincipen ska en kommun behandla alla sina medlemmar likvärdigt (Kommunallagen 1991:900). Detta förutsätter att vi har utarbetade rutiner för att erbjuda likvärdig samhällsservice även till personer som av någon anledning behöver skydda sina personuppgifter.

Den enskilda personen har ett ansvar att själv upplysa om sekretessmarkering eftersom det inte åligger en myndighet att utan anledning kontrollera om en person har sekretessmarkering i folkbokföringen. I vissa fall hämtar myndigheten uppgifter från folkbokföringen och Skatteverket när personen tar kontakt med myndigheten, i vilka det i så fall framgår om sekretessmarkering finns. IT-stöd kan även hämta information kontinuerligt för att inhämta aktuella uppgifter.

När det framgår att en person har skyddade personuppgifter ska en utredning göras för att kartlägga typen av skyddade personuppgifter och individens skyddsbehov. Utifrån utredningen ska ärendet handläggas och personuppgifterna hanteras enligt utarbetade rutiner för att säkerställa att skyddet bibehålls.

All hantering av personuppgifter ska göras på sådant sätt att skyddade personuppgifter inte röjs så det kan vara till skada för den enskilde.

> *I offentlighets- och sekretesslagen finns regler för olika myndigheters verksamheter.*
> *För att sekretessen ska gälla för personuppgifter krävs att myndighetens sekretess omfattar allmänna personuppgifter och inte endast verksamhetsspecifika uppgifter. Alla myndigheter har dock inte några "egna" sekretessbestämmelser som innebär att uppgifter om enskilda kan skyddas vid exempelvis förföljelse. Sedan den 1 oktober 2006 gäller därför en generell sekretess för alla myndigheter för adressuppgift eller annan uppgift som kan lämna upplysning om var den enskilde befinner sig, om det av särskild anledning kan antas att den enskilde eller någon denne närstående kan komma att utsättas för våld eller annat allvarligt men om uppgiften röjs. Namn omfattas inte av denna sekretessregel.*
>
> *Det finns inte någon allmän sekretessregel som gör att sekretess följer med en uppgift som lämnas från en myndighet till en annan.*

(ur Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter i offentlig förvaltning)

Under referenser i denna riktlinje kan du läsa om de lagstöd som finns för olika verksamheter.

Dokumentation

Dokumentation av personuppgifter som är skyddade ska ske på ett säkert sätt så de inte röjs. De ska dokumenteras så att bara en eller ett fåtal har tillgång till dem. Dokumentation kan till exempel ske via IT-stöd eller i pappersform, beroende på var säkerhet och åtkomstbegränsning kan garanteras och kontrolleras.

Att en person har en sekretessmarkering eller kvarskrivning innebär inte att personen kan vara anonym i sin kontakt med myndigheter. Personen ska inte registreras som en kod/"skyddad identitet"/m.m. då personens identitet är känd. Pappersakt med personuppgifter ska förvaras i låst skåp.

Myndigheter bör inte i onödan ta med formaliainformation, som t.ex. adressuppgifter eller telefonnummer, i handlingar. Det bör göras en översyn av vilken information som behöver vara med i t.ex. en ansökningshandling, beslut, protokoll eller andra handlingar. Detta för att inte i onödan sprida personuppgifter genom att en handling begärs ut eller sprids på annat sätt.

IT-stöd

Egna system får inte köpas in och personuppgiftsbiträdesavtal får inte tecknas utan att detta går via IT-avdelningen och dataskyddsombudet.

Vid utveckling och upphandling av IT-stöd ska särskild beaktan tas till hanteringen av personuppgifter särskilt beaktas. E-tjänster rekommenderas inte om inte hög säkerhet kan garanteras för personuppgifter som är skyddade. Risken att uppgifter felaktigt lämnas ut, av misstag eller medvetet, ökar med antalet personer som kan ta del av uppgifterna. IT-stödet bör utformas så att endast ett fåtal personer med särskild behörighet har tillgång till sekretessmarkerade uppgifter. Det bör på ett tydligt och enhetligt sätt framgå att uppgifter ligger under sekretessmarkering eller att personen har skyddad identitet. Det ska vara möjligt att i efterhand kontrollera vilka personer som har tagit del av skyddade personuppgifter.

Redan registrerade uppgifter

Om den skyddade uppgiften (ej personnummer) finns dokumenterad sedan tidigare då den inte var skyddad, ska uppgiften markeras och inte användas (trots personens samtycke). Om det inte är möjligt att markera uppgiften ska uppgiften döljas eller sparas på annan säker plats.

Personuppgifter som finns i något system som många har tillgång till, t.ex. planeringssystem, och som blir skyddade, ska plockas bort manuellt. Om uppgifterna ska sparas förvaras de enligt ovan regler om pappersakt.

Den som får kännedom om att en person har fått skyddade personuppgifter ansvarar för att vidarebefordra den informationen till kollegor inom myndigheten som också ska hantera personuppgifterna. Det ska sedan göras en utredning om vad som ska skyddas. Uppgifterna ska sedan hanteras enligt lokal rutin.

Kommunikation

Det ska finnas säkra rutiner för att kommunicera med och om personer med skyddade personuppgifter. Den som hanterar personuppgifter som är skyddade ska använda sig av säkra kommunikationskanaler. Säkra kommunikationskanaler är brev, elektronisk

kommunikation med hjälp av elektronisk legitimation och besök av den enskilde om han eller hon har legitimerat sig.
Kommunikation via e-post ska inte förekomma i fråga om uppgifter som omfattas av sekretess, vare sig inom eller mellan myndigheter. Kommunikation med andra myndigheter per telefon kan vara möjlig efter motringning. Telefonkontakt med den enskilde kan vara aktuell efter att en överenskommelse gjort med den enskilde hur det ska gå till.

Myndigheten bör ha kontakt med personen med skyddade personuppgifter och tillsammans bestämma hur kontakten ska skötas.

Post
För utskick till en person med skyddade personuppgifter kan en myndighet antingen använda den adressuppgift som myndigheten själv för fogar över eller använda sig av Skatteverkets förmedlingstjänst.

För att hantera förmedlingsposten tryggt och säkert har Skatteverket utarbetat en rutin för hanteringen av posten. All post som ska förmedlas ska sändas till Skatteverkets särskilda postförmedlingsadress i Göteborg. Skatteverket förmedlar alla typer av försändelser. Besök Skatteverkets hemsida, https://www.skatteverket.se/privat/folkbokforing/skyddadepersonuppgifter/postformedling för närmare information.

Utlämning av handlingar

I de fall där det finns personuppgifter som är skyddade ska en särskild sekretessbedömning göras innan utlämning av handling sker. I bedömningen ska hänsyn tas till personens risk för att lida skada och men i det specifika fallet. Kontaktuppgifter och vistelseadress är ofta av särskilt skyddsvärde. Om personen har kvarskrivning så är uppgiften om att personen i fråga vistas i kommunen ofta en skyddsvärd uppgift. Myndigheten är skyldig att lämna ut uppgifter till andra myndigheter där det följer av lag. I annat fall ska samtycke inhämtas. Personen som uppgifterna tillhör bör alltid informeras om att uppgifter har lämnats ut.

Företag och organisationer ansvarar för att deras hantering av personuppgifter är korrekt. I de fall myndigheten lämnar ut eller tar emot uppgifter från företag eller organisationer ska det vara tydligt om de innehåller skyddade personuppgifter. Myndigheten ska vara noga med att informera om detta och vad det innebär. Denna kommunikation kan förstärkas genom att gemensamma rutiner för informationsöverföring skapas där det är möjligt.

Om en uppgift felaktigt röjs ska det hanteras skyndsamt utifrån fastställd lokal rutin. Dataskyddsombudet ska omgående informeras. Dataskyddsförordningen definierar personuppgiftsincident som; en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Rutin

Arbetsrutiner ska finnas där det finns behov av dem för att säkra hanteringen av skyddade personuppgifter. En rutin bör innehålla:

- VAD - Rutinens omfattning, vad gäller rutinen?
- VEM - Ansvarsfördelning, vem är ansvarig för vad?
- HUR - Beskrivning av arbetsrutiner för hantering
- OM - Rutin för om skyddade personuppgifter röjts m.m.

Referenser

- Skatteverkets vägledning för hantering av personer med skyddade personuppgifter (2017-09-04)
  https://www.skatteverket.se/privat/folkbokforing/skyddadepersonuppgifter/hanteringavsekretessmarkeradepersonuppgifter.4.18e1b10334ebe8bc80002541.html

- Skolverkets vägledning för hantering av unga med skyddade personuppgifter (2017-09-04)
  https://www.skolverket.se/regelverk/juridisk-vagledning/unga-med-skyddade-personuppgifter-1.152127

- Socialstyrelsens information till socialtjänsten i dess arbete med personer som har skyddade personuppgifter. (2005)
  https://www.socialstyrelsen.se/Lists/Artikelkatalog/Attachments/9804/2005-1-6_200516.pdf

Lagstöd

Olika verksamhetsområden

På vissa områden råder det presumtion för sekretess för samtliga uppgifter om enskilds personliga förhållanden. Det gäller inom socialtjänsten 26 kap. 1 § OSL, hälso- och sjukvården, 25 kap. 1 § OSL och elevhälsan 23 kap. 2 § 1 st. OSL. Inom vissa områden är uppgifter om enskilds personliga förhållanden offentliga.

För det fall en person har skyddade personuppgifter finns en sekretessbestämmelse i 21 kap. 3 § OSL som är tillämplig oavsett var uppgiften förekommer.

Generell sekretessbestämmelse avseende förföljda personer, m.m.

Adress, telefon, m.m.

21 kap. 3 § OSL Sekretess gäller för uppgift om en enskilds bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde bor stadigvarande eller tillfälligt, den enskildes telefonnummer, e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med denne samt för motsvarande uppgifter om den enskildes anhöriga, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs.

Sekretessen gäller inte för uppgift om beteckning på fastighet eller tomträtt. Sekretessen gäller inte heller för uppgift i aktiebolagsregistret eller handelsregistret eller, i den utsträckning regeringen meddelar föreskrifter om det, i annat liknande register.

Sekretess gäller för uppgift om kopplingen mellan fingerade personuppgifter som en enskild har medgivande att använda enligt lagen (1991:483) om fingerade personuppgifter och den enskildes verkliga personuppgifter, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Kvarskrivning och fingerade personuppgifter

22 kap. 2 § OSL Sekretess gäller i ärende om kvarskrivning enligt folkbokföringslagen (1991:481) och i ärende enligt lagen (1991:483) om fingerade personuppgifter 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.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år. Lag (2014:304).

Överföring av sekretess

22 kap. 3 § OSL Får en myndighet en uppgift som är sekretessreglerad i 2 § från en myndighet som handlägger ärenden som avses där, blir 2 § tillämplig på uppgiften även hos den mottagande myndigheten.