



Riktlinjer för hantering av skyddade personuppgifter

Fastställd av kommundirektör genom delegationsbeslut 2023-08-04, dnr KS 23/0368



UPPLANDS-BRO
KOMMUN

Innehållsförteckning

1	Inledning	3
1.1	Syfte	3
1.2	Omfattning	3
2	Skyddsåtgärder.....	4
3	Generellt om hantering av skyddade personuppgifter i kommunen	4
3.1	Begäran om utlämnande av handling – hur gör vi när skyddade personuppgifter begärs ut?	4
3.1.1	Särskilt om sekretessprövning vid förekomst av skyddade personuppgifter.....	5
3.2	Tillgång till skyddade personuppgifter	5
3.3	IT-stöd.....	5
3.4	Ansvar för medarbetarnas kunskap.....	6
3.5	Kommunikation med personer som har skyddade personuppgifter.....	7
3.6	Anställda i kommunen som har skyddade personuppgifter	7
4	Verksamhetsspecifika rutiner	8
5	Förvaltning av riktlinjer	9
5.1	Relaterade dokument.....	9
5.2	Förvaltning	9
5.3	Förvaring.....	9
5.4	Uppföljning.....	9

1 Inledning

Skyddade personuppgifter är en samlingsrubrik för de olika skyddsåtgärder som Skatteverket kan besluta om med stöd av folkbokföringslagen (FOL). Människor som är utsatta för hot eller riskerar att utsättas för brott, förföljelser eller allvarliga trakasserier kan ansöka om skyddsåtgärder och Skatteverket kan besluta att deras personuppgifter ska skyddas.

Skyddade personuppgifter ska hanteras med mycket stor försiktighet. Enhetliga rutiner underlättar hanteringen inom den offentliga förvaltningen och minskar risken för att skyddade personuppgifter oavsiktligt lämnas ut. Skatteverket har i samråd med andra myndigheter utarbetat allmän information och vägledning för hantering av skyddade personuppgifter.¹

En förutsättning för att Skatteverkets beslut om skyddade personuppgifter ska vara effektiva är att de myndigheter som behöver hantera uppgifterna har rutiner för att upprätthålla skyddet. Skatteverket rekommenderar därför att myndigheter tar fram rutiner för hantering av skyddade personuppgifter.

Det är viktigt att regler och rutiner för skyddade personuppgifter är uppdaterade, efterlevs och respekteras. Det kan därför vara bra att utse en eller ett fåtal personer som ansvarar för att regler och rutiner regelbundet följs upp. En säker hantering av skyddade personuppgifter kräver också att personalen som hanterar uppgifterna har goda kunskaper om skyddsåtgärderna och de sekretessbestämmelser som myndigheten ska följa.

1.1 Syfte

Dessa riktlinjer har tagits fram som ett komplement till gällande lagstiftning, Skatteverkets vägledning och till kommunens övriga styrdokument inom området, till exempel informationssäkerhetspolicy². Vid en eventuell konflikt mellan statlig reglering och kommunens riktlinjer och rutiner gäller statlig reglering. Riktlinjerna har till syfte att öka tryggheten för personer med skyddade personuppgifter som förekommer inom kommunens verksamheter.

1.2 Omfattning

Alla verksamheter i kommunen omfattas av riktlinjerna och varje verksamhet ska bedöma vilka kompletterande rutiner som behövs för att säkerställa ett tillräckligt skydd för de uppgifter som hanteras inom verksamheten. Denna

¹ Vägledningen finns på Skatteverkets [hemsida](#).

² Kommunens styrande dokument finns samlade på kommunens hemsida, på sidan [Författningssamling och övergripande styrdokument](#).

riktlinje innehåller rekommendationer för vad sådana verksamhetsspecifika rutiner bör innehålla.

2 Skyddsåtgärder

När någon ansöker om skyddade personuppgifter kan Skatteverket välja mellan att registrera två olika typer av markeringar i folkbokföringsdatabasen:

Markering för skyddad folkbokföring

När hotbilden mot en person är mycket stark kan personen få skyddad folkbokföring enligt 16 § FOL. Uppgifter om den som har skyddad folkbokföring omfattas av sekretess med stöd av 22 kapitlet offentlighets och sekretesslagen (OSL) och ska normalt sett inte lämnas ut.

Sekretessmarkering

En sekretessmarkering ska betraktas som en varningssignal om behovet av att göra en noggrann skadeprovning enligt 22 kap. 1 § offentlighets- och sekretesslagen, OSL, när någon begär att få ut en sekretessmarkerad uppgift.

Sekretessmarkering och markering för skyddad folkbokföring aviseras från Skatteverket till andra myndigheter, när personuppgifter inhämtas från Skatteverket. Mottagande myndigheter ska enligt Skatteverkets vägledning i vart fall ha manuella rutiner för att hantera gällande sekretessbestämmelser. Den mottagande myndigheten väljer vilket som är det lämpligaste sättet att hantera skyddade personuppgifter i sina system.

3 Generellt om hantering av skyddade personuppgifter i kommunen

3.1 Begäran om utlämnande av handling – hur gör vi när skyddade personuppgifter begärs ut?

När en begäran om att ta del av allmänna handlingar kommer in till kommunen ska den hanteras i enlighet med kommunens Riktlinje angående begäran om allmänna handlingar. Det finns även vägledande material till stöd för den som ska hantera en sådan begäran.³

³ Kommunens styrande dokument finns samlade på kommunens hemsida, på sidan [Författningssamling och övergripande styrdokument](#). Vägledande material finns på [Portalen](#).

Skyddade personuppgifter omfattas i de flesta fall av stark sekretess. I 22 kapitlet i OSL finns bestämmelser om sekretess för uppgifter i folkbokföringen eller annan liknande registrering av befolkningen. Även andra sekretessbestämmelser kan vara aktuella, bland annat de bestämmelser om sekretess till skydd för uppgift om enskilda personliga förhållanden som finns i 21 kapitlet OSL.

Det är viktigt att det framgår tydligt om det förekommer skyddade personuppgifter i ett ärende eller i handlingar som förvaras hos kommunen, så att den som ska pröva en begäran blir uppmärksam på att en noggrann sekretessprövning ska göras.

3.1.1 Särskilt om sekretessprövning vid förekomst av skyddade personuppgifter

Markering för skyddad folkbokföring

Uppgifter om den som har skyddad folkbokföring omfattas av sekretess enligt 22 kap. 2 § OSL och ska normalt sett inte lämnas ut.

Sekretessmarkering

En sekretessmarkering är inte ett beslut om sekretess utan endast en varningssignal om att det alltid ska göras en noggrann skadeprövning enligt 22 kap. 1 § OSL när uppgifterna begärs ut. Den som gör prövningen kan behöva fråga vem som begär ut handlingen, för att kunna bedöma om handlingen kan lämnas ut till just den aktuella mottagaren.

3.2 Tillgång till skyddade personuppgifter

Risken att uppgifterna felaktigt lämnas ut ökar med antalet personer som kan ta del av uppgifterna. Kretsen av personer som har tillgång till skyddade personuppgifter ska därför begränsas så långt som möjligt. Utgångspunkten bör vara att enbart anställda som har behov av att ta del av uppgifterna för att utföra sina arbetsuppgifter ska ha tillgång till uppgifterna.

3.3 IT-stöd

Behandling av skyddade personuppgifter i kommunens IT-system ska följa Skatteverkets vägledning för hantering av skyddade personuppgifter. Det är upp till varje verksamhet att välja det lämpligaste sättet att hantera skyddade personuppgifter i sina system och inom verksamheten. I vissa fall kan manuell hantering av personuppgifterna vara säkrare, om hantering i ett IT-system bedöms innebära en risk.

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.

Möjligheten att vidta åtgärder för att skydda personuppgifter i olika IT-system kan vara begränsad med hänsyn till bland annat tekniska funktioner och de krav som ställts vid upphandling av systemen. Åtgärder i form av loggning och begränsning av åtkomst till skyddade personuppgifter ska användas i den mån det är möjligt för respektive system. Åtkomst till skyddade personuppgifter ska loggas i de IT-system där det finns möjlighet till det, för att göra det möjligt att i efterhand kontrollera vilka som tagit del av uppgifterna.

Åtkomsten till skyddade personuppgifter i IT-systemen bör begränsas, i den mån det är möjligt och lämpligt med hänsyn till tekniska förutsättningar och verksamhetens behov. Varje verksamhet ska bedöma vilka begränsningar som är lämpliga, behörighet bör som utgångspunkt inte ges till fler personer än vad som är nödvändigt för att verksamheten ska kunna upprätthålla sin service-skyldighet och övriga krav som lagstiftningen ställer på verksamheten. Verksamheten behöver också se till att de som hanterar skyddade personuppgifter har rätt kompetens för det.

Det är viktigt att kommunens verksamheter har uppdaterade och korrekta register och IT-system. Både manuellt hanterade register och IT-system måste hållas uppdaterade för att visa korrekt information.

I vissa fall kan ett fingerat namn användas i verksamhetens system, om det är möjligt och lämpligt med hänsyn till individens skyddsbehov och verksamhetens förutsättningar. Utgångspunkten ska vara 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, i de fallen kan andra skyddsåtgärder behöva vidtas.

3.4 Ansvar för medarbetarnas kunskap

Varje verksamhet bör utse en särskild person som har ansvar för att rutiner och regler för hantering av skyddade personuppgifter följs. *Informations-säkerhetssamordnare* kan i många fall vara en lämplig funktion, men varje verksamhet ska bedöma vilken funktion som är lämpligast att utse som ansvarig. Verksamheten ansvarar för att medarbetarna har goda kunskaper om regelverket för skyddade personuppgifter och om gällande sekretessbestämmelser i sin verksamhet.

3.5 Kommunikation med personer som har skyddade personuppgifter

Kommunikation med berörda personer, eller med andra myndigheter i ärenden som rör personer med skyddade personuppgifter, får endast ske 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 personen har legitimerat sig.

E-post ska *inte* användas för kommunikation av 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 personen utger sig för att vara. En sådan kontroll kan ske genom återuppringning till myndighetens officiella telefonnummer.

Vid kommunikation med enskilda via post ska Skatteverkets förmedlingstjänst användas i första hand.⁴ Detta för att minimera risken att posten skickas fel. Endast i de fall det är helt säkerställt att en adress stämmer och är aktuell kan post skickas direkt till adressen.

Det är lämpligt att bara ett fåtal personer inom en verksamhet kommunicerar med personer som har skyddade personuppgifter, eftersom det minskar risken för att känsliga uppgifter röjs.

3.6 Anställda i kommunen som har skyddade personuppgifter

Om en anställd har fått ett beslut om sekretessmarkering eller skyddad folkbokföringsadress är personen skyldig att visa upp beslutet från Skatteverket för sin arbetsgivare. Detta gäller både vid nyanställning och under pågående anställning. Detta för att säkerställa att arbetsgivaren hanterar personuppgifterna enligt rätt rutiner.

Om beslutet kommer under pågående anställning ska personalavdelningen kontaktas, för att säkerställa att personuppgifterna hanteras korrekt både gällande administration och uppgifter i HR-systemen.

⁴Information om förmedlingstjänsten finns på Skatteverkets [hemsida](#).

4 Verksamhetsspecifika rutiner

Verksamheterna i kommunen behandlar olika personuppgifter för att fullgöra sina uppdrag. Alla berörda verksamheter i kommunen ska ta fram rutiner för hur skyddade personer ska hanteras i verksamheten. Rutinerna ska utarbetas utifrån bedömningar av hur uppgifterna kan skyddas på lämpligast sätt, utifrån de förhållanden som råder i verksamheten.

Genom en riskanalys kan verksamheten klarlägga hur skyddet för uppgifter om en person med skyddade personuppgifter kan utformas och upprätthållas på lämpligast sätt. Varje verksamhet bör göra en översyn av vilken information som måste finnas med i ansökningar, beslut, protokoll, klasslistor och liknande dokument, för att undvika att få in skyddade personuppgifter i verksamhetssystem och andra former av dokumentation.

Verksamhetsspecifika rutiner ska utformas i enlighet med Skatteverkets vägledning och bör klargöra hur följande ska hanteras:

- Hur information om de skyddade uppgifterna ska nå berörd personal och vem som ansvarar för detta.
- Hur kommunikation mellan verksamheten och personer med skyddade personuppgifter ska gå till, för att säkerställa att skyddet för personuppgifterna kan upprätthållas. Om det är möjligt och lämpligt bör verksamheten ta kontakt med berörda personer för att inhämta deras önskemål om hur uppgifterna ska hanteras och hur kommunikation mellan kommunen och berörda personer ska gå till.
- Hur de skyddade uppgifterna ska hanteras i verksamhetssystemen.
- Hur anställda i verksamheten ska agera om någon utomstående frågar om en person med skyddade personuppgifter.
- Hur anställda i verksamheten ska agera om något inträffar, till exempel om någon obehörig får tillgång till skyddade personuppgifter.
- Hur uppgifter om anställda i verksamheten som har skyddade personuppgifter ska hanteras.
- Vilka åtgärder som ska vidtas när skyddsåtgärder avslutas.
- Om det finns särskilda risker som verksamheten behöver beakta, något som de anställda ska vara särskilt uppmärksamma på. Om en verksamhet till exempel behöver lämna uppgifter om en person som har skyddade personuppgifter till externa utförare ska det framgå av verksamhetens rutiner hur det kan ske på ett säkert sätt.

5 Förvaltning av riktlinjer

5.1 Relaterade dokument

Dessa riktlinjer utgör ett komplement till gällande lagstiftning, Skatteverkets vägledning och till kommunens övriga styrdokument inom området:

- Informationssäkerhetspolicy
- Personalpolicy
- Riktlinje angående begäran om allmänna handlingar
- Riktlinje vid hot och våld
- Handlings- och aktivitetsplan mot hedersrelaterat våld och förtryck
- Handlings- och aktivitetsplan mot våld i nära relation
- Vägledningar och rutiner inom området

5.2 Förvaltning

Kommunstyrelsen beslutar om riktlinjerna och ansvarar för att förvalta dokumentet, vilket innebär att säkerställa tillämpning, uppföljning och revidering vid behov.

Kommunstyrelsen ansvarar för att sprida, informera och utbilda i hantering av skyddade personuppgifter vid behov.

Riktlinjerna gäller till dess att de upphävs av kommunstyrelsen, eller ersätts av annat styrdokument som fastställts av kommunstyrelsen eller kommunfullmäktige.

5.3 Förvaring

Riktlinjerna ska publiceras på kommunens hemsida: Författningssamling och övergripande styrdokument. Administrativa avdelningen ansvarar för att riktlinjerna publiceras på hemsidan och att dokumentet tas bort från hemsidan när riktlinjerna har upphört att gälla.

5.4 Uppföljning

Kommunstyrelsen följer löpande upp riktlinjerna och reviderar dem vid behov.