Styrdokument
2025-02-02
Fastställd: Kommunstyrelsen 2025-01-28,
§ 2

Gäller för: Samtliga nämnder
Dokumentansvarig:
Informationssäkerhetssamordnare

Dnr : **KS2024/310-3**

Riktlinjer för hantering av skyddade personuppgifter

Innehållsförteckning

Innehåll

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.

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 kommuner och 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

Denna riktlinje utgör ett tillägg till gällande lagstiftning, Skatteverkets vägledning och till kommunens övriga styrdokument inom området, till exempel kommunens informationssäkerhetspolicy. 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

Samtliga förvaltningar i Bollebygds kommun omfattas av riktlinjen och där förvaltningarna ska bedöma vilka rutiner som behövs för att säkerställa ett tillräckligt skydd för de uppgifter som hanteras inom verksamheten. Respektive förvaltning ansvarar för att ta fram denna rutin. Denna riktlinje innehåller rekommendationer för vad sådana verksamhetsspecifika rutiner bör innehålla.

2 Skyddsåtgärder

Gemensamt för skyddsåtgärderna är att den enskilde lever med någon form av hotbild riktad mot sig och att skyddet ska förhindra att uppgifter om den enskilde sprids. När någon ansöker om skyddade personuppgifter kan Skatteverket välja mellan att registrera tre olika typer av markeringar i folkbokföringsdatabasen.

2.1 Skyddad folkbokföring

Då 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.

Skyddad folkbokföring ger en djupare nivå och beviljas av Skatteverket och används för att skydda personer som riskerar hot, våld eller förföljelse. Det innebär att personens adress och andra uppgifter inte är offentligt tillgängliga.

2.2 Sekretessmarkering

En sekretessmarkering ska bedömas 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 sekretessmarkerad uppgift.

2.3 Fingerade personuppgifter

Fingerade personuppgifter är en skyddsåtgärd som används för att ge en person en ny identitet, inklusive namn och personnummer, för att skydda dem från allvarliga hot mot deras liv, hälsa eller frihet. Detta beslut är en sista utväg i extrema fall, exempelvis vid hot från våldsamma relationer.

2.3.1 Aviseringar från Skatteverket

Sekretessmarkering och skyddad folkbokföring aviseras från Skatteverket till andra myndigheter, när personuppgifter inhämtas från Skatteverket. Förvaltningar inom kommunen ska ha särskilda rutiner för att hantera skyddade personuppgifter i enlighet med sekretessbestämmelser i OSL, och att välja det lämpligaste sättet för att hantera skyddade personuppgifter i sina verksamhetssystem och inom verksamheten. I vissa fall kan en manuell hantering av personuppgifterna vara säkrare om ett verksamhetsstöd bedöms innebära en risk.

Bollebygds kommuns förvaltningar ska samråda kring hur skyddade personuppgifter ska hanteras. Detta för att minska risken vid stora skillnader mellan olika rutiner som kan leda till felaktig tolkning och att uppgifter röjs.

3 Generellt om hantering av skyddade personuppgifter i kommunen

Hantering av skyddade personuppgifter är en viktig del av skyddet för individer som är utsatta för hot eller annan fara. För att trygga en korrekt hantering är kunskap och medvetenhet hos dem som hanterar dessa uppgifter avgörande, detta för att minimera risken för informationsläckor.

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 hantering av begäran om allmänna handlingar. Det finns även vägledande material till stöd för den som ska hantera en sådan begäran .

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 enskilds personliga förhållanden som finns i 21 kapitlet OSL.

Det är viktigt att det blir tydligt om det finns 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. Sekretess gäller, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till den enskilde lider men.

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 stiger med antalet personer som kan ta del av uppgifterna. Gruppen av personer som har tillgång till skyddade personuppgifter ska därför hållas nere så långt som möjligt. Utgångspunkten är att enbart medarbetare som i sitt uppdrag har behov av att ta del av uppgifterna har 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 förvaltning 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.

Huvudregeln i Bollebygds kommun är att medarbetare med skyddade personuppgifter inte ska vara offentligt eller internt sökbara. Skyddsvärda uppgifter ska behandlas med sekretess. Ansvarig chef ska tillsammans med medarbetare som fått beslut om skyddade personuppgifter göra en gemensam riskbedömning samt kartlägga vilken information som visas i kommunens IT-systemen och därefter sörja för att skyddsvärd information skyddas.

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 förvaltning 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 serviceskyldighet och övriga krav som lagstiftningen ställer på verksamheten. Förvaltningarna behöver också se till att de som hanterar skyddade personuppgifter har rätt kompetens för det.

Det är viktigt att kommunens förvaltningar 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 de förvaltningar som behandlar personuppgifter 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 Medarbetarnas kunskap

Varje förvaltning ska utse en särskild funktion som har ansvar för att rutiner och regler för hantering av skyddade personuppgifter följs. Kommunens förvaltningar ansvarar för att medarbetarna har goda kunskaper om regelverket för skyddade personuppgifter och om gällande sekretessbestämmelser i sin verksamhet. Informationssäkerhetssamordnare kan vara behjälplig i frågor som rör regelverket, dock ska varje förvaltning bedöma vilken funktion som är lämpligast att utse som ansvarig.

3.5 Kommunikation med människor som har skyddade personuppgifter

E-post ska inte användas för kommunikation av uppgifter som omfattas av sekretess, varken 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 bör man ska komma överens med den enskilde om hur denne önskar få ut sin post, genom att kommunen postar, genom att hämta ut eller genom Skatteverkets förmedlingstjänst.

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 Medarbetare i kommunen som har skyddade personuppgifter

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

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

4 Verksamhetsspecifika rutiner

Kommunens förvaltningar behandlar olika personuppgifter för att fullgöra sina uppdrag. Alla förvaltningar 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 att göra 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 skrivas i enlighet med Skatteverkets vägledning och bör visa på 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 bevaras.
- Hur de skyddade uppgifterna ska hanteras i verksamhetssystemen.
- Hur medarbetare i verksamheten ska handla 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 medarbetare i verksamheten som har skyddade personuppgifter ska hanteras.
- Vilka åtgärder som ska vidtas när skyddsåtgärder avslutas.
- Om det finns särskilda risker som verksamheten behöver tänka på, något som medarbetarna särskilt ska vara uppmärksamma på. Om en verksamhet till exempel behöver lämna uppgifter om en person som har skyddade personuppgifter till externa utförare ska det framgå av förvaltningens rutiner hur det kan ske på ett säkert sätt.

5 Förvaltning av riktlinjerna

Denna riktlinje är vägledande principer och är en kontinuerlig process som ska säkerställa att arbetet följer de gällande lagar, policys och förordningar i enlighet med mål och värderingar.

5.1 Relaterade dokument

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

- Utlämnande av allmänna handlingar
- Personalpolicy
- Riktlinje vid hot och våld
- Plan mot hedersrelaterat våld
- Plan mot våld i nära relationer
- Informationssäkerhetspolicy
- 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.

Kommundirektören har på Kommunstyrelsens uppdrag ansvaret för att sprida och implementera riktlinjen, informera och utbilda i hantering av skyddade personuppgifter vid behov.

Riktlinjerna gäller tills vidare och kan endast upphävas av kommunstyrelsen, eller ersättas av annat styrdokument som fastställts av kommunstyrelsen eller kommunfullmäktige.

5.3 Förvaring

Riktlinjerna ska publiceras på kommunens hemsida: Styrdokument - Bollebygds kommun
Administrativa avdelningen ansvarar för att riktlinjerna publiceras på hemsidan, insidan och i chefshandboken, samt att dokumentet tas bort från hemsidan när riktlinjerna har upphört att gälla.

5.4 Uppföljning

Dokumentansvarig följer löpande upp riktlinjerna och reviderar dem vid behov, därefter beslutar Kommunstyrelsen den reviderade riktlinjen.