RIKTLINJE
RIKTLINJER FÖR SKYDDADE PERSONUPPGIFTER

Diarienummer	Fastställd/senast uppdaterad	Beslutsinstans	Ansvarigt politiskt organ	Ansvarig processägare
KFKS-2024-00553	2024-06-17	Kommunfullmäktige	Kommunstyrelsen	Kanslidirektör
Riktlinje	Riktlinjer för skyddade personuppgifter			

Riktlinjer för skyddade personuppgifter

Dokumentets syfte

Syftet med riktlinjen är att säkerställa att skyddade personuppgifter hanteras på rätt sätt.

Dokumentet gäller för

Alla nämnder i kommunen och de kommunala bolagen.

Skyddade personuppgifter

Uppgifter som finns i folkbokföringen är som huvudregel offentliga. I vissa fall kan det dock skada en person om uppgifter om personen lämnas ut. Det kan till exempel gälla den som riskerar att utsättas för hot eller förföljelse. Personen kan då ansöka om skyddade personuppgifter. Skyddet ska förhindra att uppgifter om den enskilde sprids.

Det finns tre nivåer av skyddade personuppgifter:

Skyddad folkbokföring är den högsta nivån av skyddade personuppgifter som man kan ansöka om hos Skatteverket. Det innebär att den utsatta personen folkbokförs på en annan folkbokföringsort än där hen är bosatt. Det kan bli aktuellt för någon som riskerar att utsättas för brott, förföljelse eller allvarliga trakasserier. Det ställs även krav på att personen själv, utifrån sin förmåga, agerar så att skyddet får en effekt.

Sekretessmarkering är en lägre nivå av skyddade personuppgifter än skyddad folkbokföring och ställer inte samma krav på skyddets effekt. Sekretessmarkeringen ska göra det svårare för andra att ta del av en persons personuppgifter. Markeringen fungerar som en varningssignal för myndigheter vid hanteringen av den enskildes personuppgifter.

Fingerade personuppgifter kan ges i de fall en person är utsatt för allvarlig brottslighet och hotas till liv, hälsa, frihet eller frid. Det innebär att den drabbade

personen får nya identitetsuppgifter, till exempel ett nytt namn och nytt personnummer. Skyddet används enbart i undantagsfall, som en sista utväg när alla andra åtgärder är otillräckliga. Ansökan om fingerade personuppgifter görs hos Polismyndigheten.

Denna riktlinje gäller enbart skyddad folkbokföring och sekretessmarkering. Vid fingerade personuppgifter känner kommunen inte till den tidigare identiteten och det går inte heller att se att den nuvarande identiteten är fingerad.

Hantering av skyddade personuppgifter i kommunen

Eget ansvar

Den som har skyddade personuppgifter har ett eget ansvar att själv upplysa kommunen om detta.

Verksamhetsspecifika rutiner

Respektive verksamhet i kommunen ska ha interna rutiner som är anpassade utifrån verksamhetens målgrupp/kunder så att skyddade personuppgifter hanteras korrekt.

Behöriga personer

Risken för att skyddade personuppgifter lämnas ut, av misstag eller medvetet, ökar med antalet personer som har tillgång till uppgifterna. Det gäller oavsett om de läses på skärm eller på papper. Kretsen av personer som har behörighet att ta del av skyddade personuppgifter ska därför begränsas så långt som möjligt.

Åtkomsten till skyddade personuppgifter i IT-systemen/digitala verksamhetssystemen ska 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 serviceskyldighet och övriga krav som lagstiftningen ställer på verksamheten.

Det bör 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/digitala verksamhetssystem och på utskrifter.

Utbildning och kompetens

De medarbetare som hanterar skyddade personuppgifter behöver ha rätt kompetens för det. Respektive verksamhet/enhet inom kommunen ansvarar för att samtliga berörda medarbetare har goda kunskaper om regelverket för skyddade personuppgifter.

IT-stöd

Behandling av skyddade personuppgifter i kommunens IT-system/digitala verksamhetssystem ska följa Skatteverkets vägledning för offentliga aktörers hantering av skyddade personuppgifter. Det är upp till varje enhet/verksamhet att välja det lämpligaste sättet att hantera skyddade personuppgifter i sina system och inom enheten/verksamheten. I vissa fall kan manuell hantering av personuppgifterna vara säkrare, om hantering i ett IT-system/digitala verksamhetssystem bedöms innebära en risk på grund av att IT-systemet/digitala verksamhetssystemet saknar förutsättningar för lämplig säkerhet vid hantering av skyddade personuppgifter.

För att kommunen ska kunna hantera skyddade personuppgifter riskfritt ska särskild hänsyn tas till hanteringen av skyddade personuppgifter redan vid utveckling och upphandling av verksamhetsstöd.

I vissa fall kan ett fingerat namn användas i enhetens/verksamhetens system, om det är möjligt och lämpligt med hänsyn till individens skyddsbehov och enhetens/verksamhetens förutsättningar.

Dokumentation

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

Risk- och konsekvensanalys

Varje enhet/verksamhet ska ha en uppdaterad risk- och konsekvensanalys utifrån enhetens/verksamhetens målgrupp/kunder (som innehar skyddade personuppgifter). Resultatet av analysen utgör underlag för de verksamhetsspecifika rutinerna för hanteringen av skyddade personuppgifter.

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 IT-system/verksamhetssystem och andra former av dokumentation.

Kommunikation

Kommunikation med berörda personer, eller med andra myndigheter i ärenden som rör personer med skyddade personuppgifter, får endast ske via en säker kommunikationskanal. I Skatteverkets vägledning för offentliga aktörers

hantering av skyddade personuppgifter anges säkra kommunikationskanaler som Skatteverket rekommenderar.

Myndigheteter bör normalt använda förmedlingstjänsten för att skicka post till personer med skyddade personuppgifter. Detta för att minimera risken att posten skickas fel.

Det ska särskilt noteras att kommunikation inte ska ske via okrypterad e-post när det gäller skyddade personuppgifter, varken inom eller mellan myndigheter eller med personen i fråga.

Loggkontroller

Åtkomst till skyddade personuppgifter ska loggas i de IT-system/digitala verksamhetssystem där det finns möjlighet till det, för att göra det möjligt att i efterhand kontrollera vilka som tagit del av uppgifterna.

Utlämning av handlingar

När en begäran om att ta del av allmänna handlingar kommer in till kommunen ska den hanteras i enlighet med kommunens guide ”Begäran om allmän handling – en guide”. Skyddade personuppgifter omfattas i de flesta fall av stark sekretess. En sedvanlig sekretessprövning ska därför göras.

Om uppgifter röjs

Varje verksamhet måste ha beredskap för att kunna agera om skyddade personuppgifter röjs. Det är särskilt viktigt om personers säkerhet är i fara. Verksamheten bör prata med personen för att avgöra vilka åtgärder som behöver vidtas. Hur allvarlig en röjning av uppgifter är kan bland annat bero på vilken typ av uppgifter det gäller, hur många som har fått sina uppgifter röjda, och till vem eller vilken myndighet uppgifterna har röjts.

Om uppgifter har röjts ska verksamheten oftast omgående informera berörda personer och andra myndigheter om incidenten. Särskilt viktigt är det att informera Skatteverket, eftersom incidenten kan påverka beslutet om skyddade personuppgifter.

En röjning av skyddade personuppgifter utgör en personuppgiftsincident enligt dataskyddsförordningen.

Uppföljning

Kommunstyrelsen är ansvarig för att löpande följa upp riktlinjerna och dess efterlevnad.