DET HÄR ÄR ETT STYRDOKUMENT

RIKTLINJE

Hantering av skyddade personuppgifter

BOTKYRKA LÅNGT IFRÅN LAGOM BOTKYRKA

Dokumentkategori:	Normerande
Beslutat av:	Kommunstyrelsen
Antagen:	2025-12-08
Diarienummer:	KS/2025:00295
Dokumentet gäller för:	Samtliga nämnder och förvaltningar
Dokumentansvarig	Kommunstyrelsen
Ansvar för revidering:	Dataskyddsombud

BOTKYRKA KOMMUN

BOTKYRKA KOMMUN

Kommunstyrelsen Dnr: KS/2025:00295

2025-10-22

Riktlinje för hantering av skyddade personuppgifter i Botkyrka kommun

Innehållsförteckning

Bakgrund

Personuppgifter som finns i folkbokföringen är som huvudregel offentliga. En person som är under hot eller förföljelse kan få skyddade personuppgifter. 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.

På varje förvaltning behöver det utses en eller ett fåtal personer som ansvarar för att regler och rutiner regelbundet följs upp. En säker hantering av skyddade personuppgifter kräver också att medarbetare som hanterar uppgifterna har goda kunskaper om skyddsåtgärderna och de sekretessbestämmelser som myndigheten ska följa.

Syfte

Syftet med riktlinjen är att säkerställa att Botkyrka kommun hanterar skyddade personuppgifter på ett tryggt, lagligt och enhetligt sätt för att minimera risken för att information röjs och att den enskilde lider skada.

Denna riktlinje har tagits fram som ett komplement till gällande lagstiftning, Skatteverkets vägledning och till kommunens övriga styrdokument inom området, till exempel kommunens Riktlinje för dataskydd och hantering av personuppgifter.[2]

[1] Skatteverket vägledning

[2] Riktlinje dataskydd Dnr KS/2023:00743

Omfattning

Riktlinjen gäller samtliga förvaltningar inom Botkyrka kommun. Ansvaret för att revidera och hålla riktlinjen uppdaterad ligger på kommunstyrelseförvaltningen, avdelningen för ekonomi och kansli. Riktlinjen gäller alla kategorier av personer, inklusive förtroendevalda.

Inledning

Enhetliga rutiner underlättar hanteringen inom den offentliga förvaltningen och minskar risken för att skyddade personuppgifter oavsiktligt lämnas ut. Skatteverket har därför i samråd med andra myndigheter utarbetat en allmän information och vägledning för hantering av skyddade personuppgifter. Kommunen ska följa Skatteverkets vägledning för offentliga aktörers hantering av skyddade personuppgifter.

Information om skyddsåtgärder och hur enskilda kan få stöd finns på Skatteverkets webbplats eller genom kontakt med myndigheten. 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.

Nivåer av skyddade personuppgifter

Det finns tre nivåer av skyddade personuppgifter:

- Sekretessmarkering
- Skyddad folkbokföring
- Fingerade personuppgifter

Denna riktlinje gäller enbart sekretessmarkering och skyddad folkbokföring. Vid fingerade personuppgifter känner kommunen inte till den tidigare identiteten och det går inte heller att se att den nuvarande identiteten är fingerad, men det kan vara bra att ha kännedom om begreppet.

De olika nivåerna beskrivs närmare nedan.

Sekretessmarkering

En sekretessmarkering är en lägre nivå av skyddade personuppgifter än skyddad folkbokföring och ställer inte samma krav på skyddets effekt. En sekretessmarkering registreras i folkbokföringsdatabasen och aviseras via Navet. Markeringen är enbart en varningssignal om behovet av att göra en noggrann skadeprövning när någon begär att få ut en sekretessmarkerad uppgift.

Skyddad folkbokföring

Skyddad folkbokföring är den högsta nivån av skyddade personuppgifter som man kan ansöka om hos Skatteverket. Skyddad folkbokföring 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. Om en person har skyddad folkbokföring framgår inte den verkliga vistelseorten av folkbokföringen och sprids inte heller till andra myndigheter via Navet.

Fingerade personuppgifter

Om en person är utsatt för särskilt allvarlig brottslighet som riktar sig mot personens liv, hälsa, frihet eller frid kan personen få fingerade personuppgifter. Det innebär att personen får nya identitetsuppgifter, till exempel ett nytt namn och nytt personnummer. Fingerade personuppgifter godkänns av Polismyndigheten och skickas sedan över till Skatteverket. Det innebär alltså att du som medarbetare i kommunen inte kommer ha kännedom om någon har en ny identitet. Om de behöver stöd genom kommunal service är det ofta polisen som först tar kontakt.

Matris över begreppen

Kategorier	***Sekretessmarkering***	***Skyddad folkbokföring***	***Fingerade uppgifter***
Gäller	En eller flera personuppgifter	Uppgift om adress och uppgifter som kan kopplas ihop och leda till folkbokföringsadress	Alla personuppgifter
Innebär	Det ska utredas vilka uppgifter som är skyddsvärda. Kräver alltid en sekretessbedömning vid utlämning.	Personen bor på en adress som inte är den som är folkbokförd. Skatteverket förmedlar posten.	En helt ny identitet, endast Polismyndigheten vet kopplingen.
Meddelas	Skatteverket gör en sekretessmarkering i folkbokföringsbasen som syns i Navet. Personen har en skyldighet att informera om sin sekretessmarkering.	Skatteverket gör en sekretessmarkering och personen folkbokförs i en kommun där personen inte bor, den verkliga adressen syns inte i Navet.	Den nya identiteten meddelas inte någonstans. Medarbetare kommer inte ha kännedom om att det är en fingerad identitet.
Ansöker hos	Skatteverket	Skatteverket	Polismyndigheten
Regleras av	22 kap. 1 § OSL 21 kap. 3 § OSL	16 § Folkbokföringslagen (1991:481), FOL 22 kap. 2 och 3 §§ OSL	Lag (1991:483) om fingerade personuppgifter

Ansvar

Respektive nämnd och styrelse är personuppgiftsansvarig för de behandlingar av personuppgifter som sker inom nämndens och styrelsens ansvarsområde. Detta innebär även att nämnden och styrelsen har ett ansvar för att deras förvaltning hanterar skyddade personuppgifter på ett lagenligt sätt. Riktlinjen ska göras känd inom kommunen via de ansvariga medarbetarna. Förvaltningsledningen har i uppdrag att tillse att riktlinjen görs känd, att nyanställda medarbetare informeras samt att följa upp hanteringen av skyddade personuppgifter.

Kommunstyrelsen ansvarar för övergripande riktlinjer och säkerhetsrutiner.

Nämnden ansvarar för att kartlägga behov av lokala rutiner. Varje nämnd ansvarar för att lokala rutiner för hantering av personuppgifter tas fram samt säkerställer att denna riktlinje efterlevs. En rutin ska innehålla en sammanställning av åtgärder som ska vidtas när en person med skyddade personuppgifter hanteras.

Verksamhetschefer ansvarar för att riktlinjer följs inom sina enheter och att medarbetare får relevant utbildning. Dataskyddsombudet säkerställer att behandling av skyddade personuppgifter följer dataskyddsförordningen (GDPR) och annan relevant dataskyddslagstiftning i enlighet med kommunens dataskyddspolicy och riktlinjen för dataskydd.

Alla medarbetare som hanterar personuppgifter ska vara informerade och uppdaterade om rutiner och skyldigheter kring hanteringen av skyddade personuppgifter.

Hantering av skyddade personuppgifter i kommunen

Personuppgiftsansvarig

Varje nämnd och styrelse inom Botkyrka kommun är personuppgiftsansvarig för de behandlingar av de personuppgifter som görs inom de egna nämndernas verksamheter. Ansvaret innefattar att vidta lämpliga tekniska och organisatoriska åtgärder för att hantera alla personuppgifter som behandlas. Säker och riskminimerande hantering av

skyddade personuppgifter förutsätter både trygga IT-system och begränsad åtkomst för medarbetare.

Varje verksamhet/förvaltning ska utse minst en medarbetare med ansvar för att säkerställa att rutiner och regler för hantering av skyddade personuppgifter följs. Medarbetaren ska regelbundet övervaka och följa upp efterlevnaden.

Medarbetare som hanterar skyddade personuppgifter ska ha mycket god kunskap om rutinerna för hanteringen av uppgifter med skyddad folkbokföring eller sekretessmarkering.

Eget ansvar

En person som har skyddade personuppgifter har ett ansvar att själv upplysa kommunen om egen sekretessmarkering. Denne har även ett eget ansvar att skydda uppgifter om sig själv som anses vara skyddsvärda.

Behöriga personer

Enligt principen om minsta möjliga behörighet ska antalet medarbetare som har behörighet att ta del av skyddade personuppgifter begränsas så långt som möjligt. Åtkomsten ska även vid behov vara tidsbegränsad.

Tillgången till skyddade personuppgifter i IT-system eller andra digitala system inom kommunen ska begränsas för att minska risken av spridning av de skyddade personuppgifterna. För att effektivt styra åtkomsten ska en rollbaserad behörighetsmodell användas, där behörigheter tilldelas utifrån fördefinierade roller, exempelvis handläggare, administratör eller teknisk support. Dessa roller ska regelbundet granskas och uppdateras för att säkerställa att rätt användare har rätt åtkomstnivå.

För att förhindra obehörig åtkomst ska stark autentisering användas vid inloggning till system där skyddade personuppgifter hanteras. Det innebär att tvåfaktorsautentisering ska tillämpas, och att kommunens mål är att varje användare har ett individuellt konto. Delade konton bör inte användas i dessa system förutom när det är absolut nödvändigt.

Behörighetsåtkomst i IT-system och tjänster

Hantering av skyddade personuppgifter i kommunens IT-system ska följa Skatteverkets vägledning för hantering av skyddade personuppgifter. IT-

system och tjänster ska konfigureras enligt principerna om informationssäkerhet, dataskydd och sekretess. Varje förvaltning ansvarar för att välja det mest lämpliga sättet att hantera skyddade personuppgifter både inom sina system och inom förvaltningen.

I säkra IT-system och andra digitala verktyg inom kommunen där det förekommer personuppgifter ska det på ett tydligt sätt framgå för den behörige användaren att uppgifterna är markerade för skyddad folkbokföring eller har sekretessmarkering. Detta gäller även för utskrifter.

För att kommunen ska kunna hantera skyddade personuppgifter på ett så riskfritt sätt som möjligt ska särskild hänsyn tas till hanteringen av skyddade personuppgifter redan vid utveckling och upphandling av verksamhetssystemet.

Loggning av utförda aktiviteter och händelser utgör en viktig del av säkerheten i alla system. Det ska vara möjligt att i efterhand kontrollera vilka medarbetare som har tagit del av skyddade personuppgifter.

Vid avslutad anställning eller förändrade arbetsuppgifter ska behörigheter omedelbart återkallas för att minimera risken för obehörig åtkomst.

Det är fördelaktigt att utformningen av dessa skyddsåtgärder ser likadana ut i alla system.

För medarbetare och förtroendevalda med skyddade personuppgifter

Om en medarbetare eller förtroendevald har fått ett beslut om sekretessmarkering eller skyddad folkbokföringsadress kan medarbetaren behöva informera sin arbetsgivare om det. Detta gäller både vid nyanställning och under pågående anställning för att säkerställa att personuppgifterna hanteras enligt gällande rutiner. Om beslutet om sekretessmarkering eller skyddad folkbokföringsadress fattas under pågående anställning ska HR-avdelningen informeras, så att korrekta åtgärder vidtas både i administrationen och i HR-systemen. Ansvarig chef ska tillsammans med medarbetaren göra en gemensam riskbedömning samt kartlägga vilken information som visas i kommunens IT-system och därefter se till att skyddsvärda uppgifter skyddas.

Omyndiga barn och elever med skyddade personuppgifter

Omyndiga barn och elever med skyddade personuppgifter påverkas på olika sätt, beroende på orsaken till skyddet och hur länge det har varit i kraft. Det är avgörande att både barnet eller eleven och deras vårdnadshavare känner sig trygga i verksamheten. Barn och unga kan i många fall inte själva bevaka sitt skydd och är därför en stor riskgrupp. Det är aldrig ett barns skyldighet att berätta om skyddade personuppgifter, utan det är ett vuxenansvar.

Dessa barn kan ha bevittnat eller själva utsatts för våld. I dessa fall behöver det göras en strikt riskbedömning. Så få som möjligt bör ha tillgång till kontaktuppgifter till vårdnadshavare och släktingar.

Kommunikation

Kommunikation med personer som har skyddade personuppgifter, eller med andra myndigheter/aktörer i ärenden som rör personer med skyddade personuppgifter, får endast ske via säkra kommunikationskanaler. I Skatteverkets vägledning för offentliga aktörers hantering av skyddade personuppgifter anges säkra kommunikationskanaler som Skatteverket rekommenderar.

Enligt Skatteverket är säkra kommunikationskanaler följande:

- brev, genom förmedlingstjänst (se nedan),
- säker elektronisk kommunikation (exempelvis digital brevlåda),
- telefon (efter motringning),
- och besök av den enskilde om denne har legitimerat sig.

Kommunen bör använda Skatteverkets förmedlingstjänst för att skicka post till personer med skyddade personuppgifter. Detta för att minimera risken att posten sprids på fel sätt, till fel ställe eller till obehörig. Skatteverkets förmedlingstjänst innebär att de ska förmedla post, via en postoperatör, till den som har skyddade personuppgifter

Kommunikation gällande skyddade personuppgifter ska alltid ske via krypterad e-post, både inom och mellan kommuner/myndigheter. Detsamma gäller för kontakt via e-post med personen som har skyddade personuppgifter.

Kommunen och myndigheter bör samverka och föra en dialog både sinsemellan och med personen som har skyddade personuppgifter för att fastställa den mest lämpliga kommunikationskanalen för att minska risken att uppgifter sprids på fel sätt.

Incidenthantering

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 närmaste chef informeras och oftast omgående ska även berörda personer och andra myndigheter informeras om incidenten. Särskilt viktigt är det att informera Skatteverket, eftersom incidenten kan påverka beslutet om skyddade personuppgifter.

En röjning av uppgifter kan också vara en personuppgiftsincident enligt dataskyddsförordningen, kontakta därför alltid förvaltningens dataskyddssamordnare och kommunens dataskyddsombud.

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.

Utlämnande av allmänna handlingar

Om allmänna handlingar begärs ut som innehåller skyddade personuppgifter ska alltid en sekretessbedömning ske. 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.

Inom folkbokföringen ska en prövning ske enligt 22 kap. 1 § Offentlighets- och sekretesslag (2009:400) (OSL) när någon begär ut uppgifter om en person med sekretessmarkering.

Sekretessen för uppgifterna i folkbokföringsdatabasen gällande den som har skyddad folkbokföring regleras i 22 kap. 2 § OSL. Som utgångspunkt gäller sekretess. Uppgifter kan endast kan lämnas ut om det står klart att den enskilde eller någon närstående inte kan lida men av utlämnandet.

Kontakta kommunjuristerna vid osäkerhet eller om det finns behov av stöd vid ett utlämnande.

Rutin på förvaltningsnivå

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

Kommunen ska ha rutiner för att följa upp hur sekretessbestämmelserna i OSL följs och om det finns säkerhetsrisker i hanteringen av skyddade personuppgifter. Ett säkert verksamhetsstöd ska till exempel logga alla händelser och transaktioner, så att både internt och externt IT-stöd i efterhand kan spåra vem som har tagit del av uppgifter om en person med skyddade personuppgifter.

Kommunens dataskyddsombud och dataskyddssamordnare ska regelbundet följa upp att regler och rutiner för skyddade personuppgifter är uppdaterade, efterlevs och respekteras enligt kommunens styrdokument för dataskydd.