Karlshamns kommun

FÖRFATTNINGSSAMLING

Beslutad av: Kommunstyrelsen
Dokumenttyp: Riktlinjer
Diarienummer: KS 2025/499
Antagna: KS § 107, 2026-04-07
Gäller från: 2026-04-09
Reviderade:
Gäller för: Samtliga förvaltningar

Riktlinjer för hantering av personer med skyddade personuppgifter

Inledning och syfte

Information om namn, personnummer, adress och andra uppgifter i folkbokföringen är som huvudregel offentliga enligt lag. För vissa personer kan ett röjande av dessa uppgifter innebära ett direkt hot mot liv, hälsa eller trygghet. Det gäller individer som lever under hot om våld, förföljelse eller annan allvarlig utsatthet. Dessa personer kan ansöka om skyddade personuppgifter hos Skatteverket i form av sekretessmarkering eller skyddad folkbokföring.

Denna riktlinje beskriver hur Karlshamns kommun ska hantera personuppgifter för personer med skyddade personuppgifter på ett rättssäkert, informationssäkert och enhetligt sätt. Den vänder sig till samtliga förvaltningar och verksamheter i kommunen och omfattar såväl organisatoriska som tekniska skyddsåtgärder och ansvarsfördelning.

Syftet är att minimera risken för att skyddade uppgifter röjs, av misstag eller bristande kännedom, och därigenom förhindra att enskilda utsätts för allvarlig skada. Riktlinjen grundar sig på dataskyddsförordningen (GDPR), offentlighets- och sekretesslagen (2009:400) (OSL), arkivlagen (1990:782) samt vägledningar från Skatteverket och Integritetsskyddsmyndigheten (IMY).

Varje verksamhet ansvarar för att ta fram lokala rutiner utifrån denna riktlinje, anpassade till aktuella system och arbetsprocesser. Informationssäkerhet och sekretess är ett gemensamt ansvar, och särskilt viktigt i hanteringen av de personer som förlitar sig på att kommunen skyddar deras uppgifter.

Olika nivåer av skyddade personuppgifter

Det finns tre nivåer av skyddade personuppgifter: fingerade personuppgifter, skyddad folkbokföring och sekretessmarkering. Polismyndigheten ansvarar för fingerade personuppgifter, medan Skatteverket ansvarar för skyddad folkbokföring och sekretessmarkering. I denna riktlinje syftar begreppet skyddade personuppgifter på skyddad folkbokföring och sekretessmarkering. Fingerade personuppgifter innebär att personer får helt nya identitetsuppgifter som gör att det inte går att spåra den tidigare identiteten, varför dessa faller utanför denna riktlinje. Kommunens inställning är att det inte görs någon skillnad i hanteringen utifrån om den enskilde har skyddad folkbokföring eller sekretessmarkering.

Skyddad folkbokföring

Skyddad folkbokföring är den högsta nivån av skyddade personuppgifter som kan ansökas om hos Skatteverket, och används för personer som riskerar att utsättas för brott, förföljelse eller allvarliga trakasserier. För att skyddet ska vara effektivt måste personen vidta åtgärder, som att flytta från en känd adress. Med skyddad folkbokföring anges inte personens verkliga adress i folkbokföringen och delas inte med andra myndigheter via Navet. Personen folkbokförs i stället under rubriken "På kommunen skriven" och Skatteverkets adress används som postadress, utan att avslöja att det är en myndighetsadress. Skatteverket hanterar och vidarebefordrar all post till personens faktiska adress.

Sekretess gäller för uppgift som ensam eller i kombination med andra kan lämna uppgifter om var en person bor eller vistas, exempel på sådana uppgifter är namn, personnummer, e-

postadress, telefonnummer, anhöriga, arbetsgivare, skola, vårdgivare och namnbyte. Observera att dessa exempel inte är uttömmande.

Sekretessmarkering

Sekretessmarkering är en lägre nivå av skydd än skyddad folkbokföring och ställer inte samma krav på åtgärder för att skyddet ska vara effektivt. Den ges till personer som inte uppfyller kraven för skyddad folkbokföring men som ändå riskerar att skadas om deras uppgifter lämnas ut. Sekretessmarkeringen registreras i folkbokföringsdatabasen och delas via Navet. Vissa myndigheter kan se både sekretessmarkeringen och personens övriga uppgifter, medan andra endast får information om att en sekretessmarkering finns tillsammans med personnumret.

Hantering av skyddade personuppgifter

Skyddade personuppgifter kan hanteras antingen i digitala system eller analogt på papper. Oavsett hanteringssätt gäller samma krav på sekretess och informationssäkerhet.

Varje verksamhet ska ta ställning till vilket hanteringssätt som är mest lämpligt för skyddade personuppgifter inom ramen för den aktuella personuppgiftsbehandlingen. Det innebär att verksamheten behöver avgöra om uppgifterna ska hanteras digitalt, analogt eller genom en kombination av båda.

Ställningstagandet ska baseras på en riskanalys och en konsekvensbedömning avseende dataskydd. Dessa bedömningar behöver inte göras för varje enskild individ med skyddade personuppgifter, utan genomförs på övergripande nivå. Det kan till exempel handla om en bedömning kopplad till ett visst IT-system eller en specifik process där skyddade personuppgifter kan förekomma.

Analog hantering

Pappersdokument med skyddade personuppgifter ska alltid hanteras med stor försiktighet. Den fysiska säkerheten är viktig och det krävs stor aktsamhet vid hantering.

Vid analog hantering gäller följande grundläggande krav:

- Märkning att uppgifterna omfattas av sekretess
- Förvaring i låst skåp, arkiv eller annat utrymme med åtkomstbegränsning
- Fysisk transport inom kommunen ska ske personligen eller genom att handlingen läggs i ett förslutet kuvert
- Kopiering och utskrift begränsas till nödvändiga fall och sker under uppsikt
- Handlingar som inte ska bevaras kastas omedelbart i sekretesskärl
- Dokument får inte lämnas obevakade eller exponeras för obehöriga, till exempel genom att ligga öppet i rum där andra vistas eller lämnas i gemensamma skrivare.

IT-system och digitala tjänster

Skyddade personuppgifter ställer särskilda krav på de digitala system och tjänster som används. Dessa krav ska beaktas redan i samband med upphandling, införande och utveckling av system.

Alla system som hanterar eller planerar att hantera skyddade personuppgifter ska genomgå:

- en riskanalys,
- en konsekvensbedömning enligt dataskyddsförordningen,
- en teknisk säkerhetsanalys där systemets funktioner granskas mot kraven för IT- och informationssäkerhet.

Den tekniska säkerhetsanalysen syftar till att säkerställa att systemet uppfyller grundläggande skyddsåtgärder för att förhindra obehörig åtkomst, röjande eller annan olämplig behandling av skyddade personuppgifter. Kommunen använder en särskild checklista för denna analys, se *Checklista: teknisk säkerhetsanalys för IT-system som hanterar skyddade personuppgifter*.

Vid varje större systemuppdatering eller förändring ska en kontroll göras för att säkerställa att skyddsnivån upprätthålls. Det ska även kartläggas hur information flödar mellan system och säkerställas att skyddet för känsliga uppgifter inte går förlorat vid överföring eller integrationer.

Skyddade personuppgifter får inte behandlas i molntjänster utan särskild bedömning och godkännande.

Åtkomst och behörighet

Personuppgifter som rör personer med skyddade personuppgifter ska endast hanteras av ett fåtal, särskilt utsedda personer inom verksamheten. Åtkomst till uppgifter om personer med skyddade personuppgifter ska begränsas enligt principen om minsta åtkomst. Det innebär att endast den som absolut behöver uppgifterna för att utföra sina arbetsuppgifter får tillgång till dem. Detta gäller oavsett om uppgifterna hanteras digitalt eller i pappersform. Åtkomsten bör med fördel dokumenteras.

Handlingsplan

I vissa fall bör en individuell handlingsplan upprättas i samråd med den enskilde. Det är särskilt aktuellt när kommunen har eller förväntas ha en varaktig kontakt med personen, exempelvis om det rör en elev, brukare, klient eller medarbetare.

Syftet med handlingsplanen är att kartlägga eventuella risker för att personens skyddade uppgifter röjs samt att fastställa vilka skyddsåtgärder som behöver vidtas.

I planen ska det även göras en överenskommelse om hur dokumentation i ärendet ska hanteras. Vuxna har i regel rätt att själva fatta beslut om hanteringen av sina personuppgifter, inklusive om uppgifter får dokumenteras under alias, i klarspråk eller i särskilda system. När

det gäller barn ska hänsyn tas till barnets ålder och mognad vid bedömningen av om barnet själv kan fatta sådana beslut. I normalfallet krävs vårdnadshavarens medverkan.

Handlingsplanen ska vara skriftlig och undertecknas av både den enskilde och ansvarig tjänsteperson.

Om personen redan har uppgifter registrerade hos kommunen, ska dessa beaktas i arbetet med att ta fram handlingsplanen och i bedömningen av hur uppgifterna fortsatt ska hanteras.

Handlingsplanen bör omfatta:

- **Kontaktvägar**: Överenskommelse om godkända kommunikationssätt (t.ex. telefon, e-post, post) och vilka adresser eller nummer som ska användas.
- **Informationsdelning**: Klargörande av vilka uppgifter som får delas internt och med externa parter, samt under vilka förutsättningar.
- **Dokumentation**: bestämma hur uppgifter ska hanteras, inklusive användning av alias eller korrekt namn.
- **Ansvarsfördelning**: Utnämning av kontaktperson inom kommunen och specificering av ansvariga för olika delar av handlingsplanen.
- **Uppföljning**: Tidsplan för regelbunden översyn och uppdatering av handlingsplanen, särskilt vid förändringar i individens situation eller skyddsnivå.
- **Incidenthantering**: Plan för vad som ska göras om uppgifter röjs eller misstänks ha röjts.

Säker kommunikation med och om personer med skyddade personuppgifter

Kommunen får endast kommunicera med personer som har skyddade personuppgifter via den eller de kontaktvägar som personen själv har godkänt. Normalt sker detta genom den särskilda kontaktväg som Skatteverket har anvisat.

Det är verksamhetens ansvar att försäkra sig om att korrekt kontaktväg används, samt att all kommunikation med den enskilde dokumenteras på ett säkert sätt.

På alla sätt där kommunen erbjuder inkommen kommunikation från enskilda (till exempel vid ansökningar, inlämning av handlingar eller kontaktformulär), ska det finnas tydlig information om hur personer med skyddade personuppgifter ska gå till väga för att ta kontakt med kommunen på ett säkert sätt.

Kommunikation med andra än den enskilde, exempelvis med andra myndigheter eller internt inom kommunen, ska ske via säkra kontaktvägar. Vid telefonsamtal med myndigheter eller andra externa aktörer bör motringning till etablerad tjänstetelefon tillämpas. Elektronisk kommunikation ska alltid ske via säker, krypterad kanal.

Incidenthantering

Om uppgifter om en person med skyddade personuppgifter misstänks ha röjts, ska den upprättade handlingsplanen aktiveras omedelbart.

Händelsen ska hanteras som en personuppgiftsincident enligt dataskyddsförordningen (artikel 33–34 GDPR). Det innebär att incidenten ska dokumenteras, bedömas och vid behov anmälas till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från det att kommunen blev medveten om den.

Den enskilde ska informeras så snart som möjligt, så att hen ges möjlighet att vidta egna skyddsåtgärder. Eftersom röjandet av skyddade personuppgifter kan utgöra ett direkt hot mot individens säkerhet, är en skyndsam hantering avgörande.

Vid incidenter av detta slag ska berörda myndigheter informeras. Det gäller särskilt Skatteverket, eftersom händelsen kan påverka beslutet om skyddade personuppgifter.

Gallring och arkivering

Gallring och arkivering ska ske i enlighet med gällande lagar, rutiner och antagen dokumenthanteringsplan.

Om analoga handlingar som innehåller skyddade personuppgifter ska arkiveras, ska dessa förvaras i en separat arkivbox. Boxen ska märkas med uppgift om att den innehåller skyddade personuppgifter. Överlämningen till arkiv ska ske personligen av handläggaren, och får inte ske via internpost eller på annat sätt.

Myndighetsutövning

Utgångspunkten är att namn och titel ska framgå på den som har fattat ett beslut. Detsamma gäller den som beslutet angår, korrekt namn behöver finnas med i beslutet.

Medarbetare som arbetar med myndighetsutövning har alltså i regel inte möjlighet att arbeta under alias.

Bilaga 1 – Checklista: teknisk säkerhetsanalys för IT-system som hanterar skyddade personuppgifter

Syfte

Checklistan fungerar som ett stöd för att granska om ett system uppfyller de tekniska säkerhetskrav som krävs för att behandla skyddade personuppgifter på ett säkert sätt.

När den ska användas

- Vid upphandling av nya system
- Vid större förändringar i befintliga system
- Vid återkommande översyn av befintliga system

1. Åtkomst- och behörighetsstyrning

- ☐ Har systemet stöd för individuell inloggning med minst tvåfaktorsautentisering (MFA)?
- ☐ Är behörigheter behovsstyrda (need-to-know)?
- ☐ Går det att begränsa åtkomst till skyddade uppgifter specifikt, t.ex. via särskilda roller?
- ☐ Går det att spärra visning av vissa uppgifter även för systemadministratörer?

2. Märkning och sekretessmarkör

- ☐ Kan uppgifter om skyddade personuppgifter tydligt märkas i systemet?
- ☐ Finns det en teknisk signal eller varning vid åtkomst av sådana uppgifter?

3. Kryptering

- ☐ Är all lagring av skyddade personuppgifter krypterad (i vila)?
- ☐ Är all överföring av skyddade personuppgifter krypterad (i rörelse)?
- ☐ Går det att dokumentera och kontrollera vilka krypteringsmetoder som används?

4. Loggning och spårbarhet

- ☐ Loggas alla åtkomster till skyddade personuppgifter?
- ☐ Går det att särskilja åtkomst till skyddade uppgifter från övriga?
- ☐ Finns funktionalitet för regelbunden granskning av loggar?
- ☐ Kan loggar sparas i enlighet med kommunens logghanteringsrutin?

5. Uppdateringar och ändringshantering

- ☐ Finns rutiner för att granska säkerhetsfunktioner vid varje större systemuppdatering?
- ☐ Säkerställs att skyddade uppgifter inte exponeras vid versionsförändringar?

6. Informationsflöden och integrationer

- ☐ Är informationsflöden till/från andra system kartlagda?

- ☐ Kan skyddade personuppgifter blockeras från att flöda till externa system?
- ☐ Säkerställs att skydd inte går förlorat i integrationer?

7. Systemets övriga skyddsåtgärder

- ☐ Finns säkerhetskopiering som omfattar även skyddade uppgifter?
- ☐ Är backuper krypterade och åtkomstskyddade?
- ☐ Finns dokumentation över tekniska skyddsåtgärder?

Bilaga 2 – Checklista: Handlingsplan för personer med skyddade personuppgifter

Syfte

Att säkerställa att personens uppgifter hanteras i enlighet med gällande lagstiftning och i enlighet med individens behov och valda skyddsnivå.

När den ska användas

- Vid längre kontakt med person som har skyddade personuppgifter (t.ex. elev, brukare, klient, medarbetare).
- Vid ny kontakt eller förändringar i skyddsnivå eller livssituation.

1. Inledning och samråd

- ☐ Har behovet av en handlingsplan bedömts utifrån kontaktens varaktighet och känslighet?
- ☐ Har samtal förts med den enskilde om vilka risker som finns och vilka alternativ som finns för skydd?
- ☐ Har det säkerställts att individen förstår vad handlingsplanen innebär?

2. Kontaktvägar

- ☐ Har överenskommelse gjorts om godkända sätt att kommunicera (telefon, e-post, post)?
- ☐ Har specifika kontaktuppgifter (nummer, adresser) dokumenterats?
- ☐ Har det säkerställts att kommunen inte använder folkbokföringsadressen eller osäkra kanaler?

3. Informationsdelning

- ☐ Har det specificerats vilka uppgifter som får delas internt?
- ☐ Har det specificerats om och när uppgifter får delas med andra myndigheter eller aktörer?
- ☐ Har förutsättningar för informationsdelning (t.ex. samtycke, rättslig grund) dokumenterats?

4. Dokumentation

- ☐ Har det tydliggjorts om uppgifter ska dokumenteras under alias, initialer eller korrekt namn?
- ☐ Har överenskommelse om vilket system eller vilken dokumentationsplats som ska användas dokumenterats?
- ☐ Har eventuella spärrar eller begränsningar i åtkomst noterats?

5. Ansvar och kontaktperson

- ☐ Har en fast kontaktperson i kommunen utsetts?
- ☐ Har kontaktpersonens namn och funktion dokumenterats i planen?
- ☐ Har ansvarsfördelning mellan olika aktörer tydliggjorts?

6. Uppföljning

- ☐ Har datum för regelbunden uppföljning och revidering av handlingsplanen bestämts?
- ☐ Har ansvarig för uppföljning utsetts?
- ☐ Har det tydliggjorts att handlingsplanen ska uppdateras vid förändrad skyddsnivå eller livssituation?

7. Incidenthantering

- ☐ Har det dokumenterats vad som ska göras vid misstänkt röjande?
- ☐ Har ansvarsfördelning vid incident tydliggjorts (ex. vem kontaktar Skatteverket, IMY)?
- ☐ Har det säkerställts att individen vet hur denne själv kan agera vid röjande?

8. Underskrift

- ☐ Har både den enskilde och ansvarig tjänsteperson undertecknat handlingsplanen?
- ☐ Har en kopia getts till den enskilde (om så önskas och är säkert)?
- ☐ Har planen diarieförts och/eller lagrats på ett säkert sätt enligt instruktion?