Göteborgs Stad

Göteborgs Stads rutin för hantering av skyddade personuppgifter

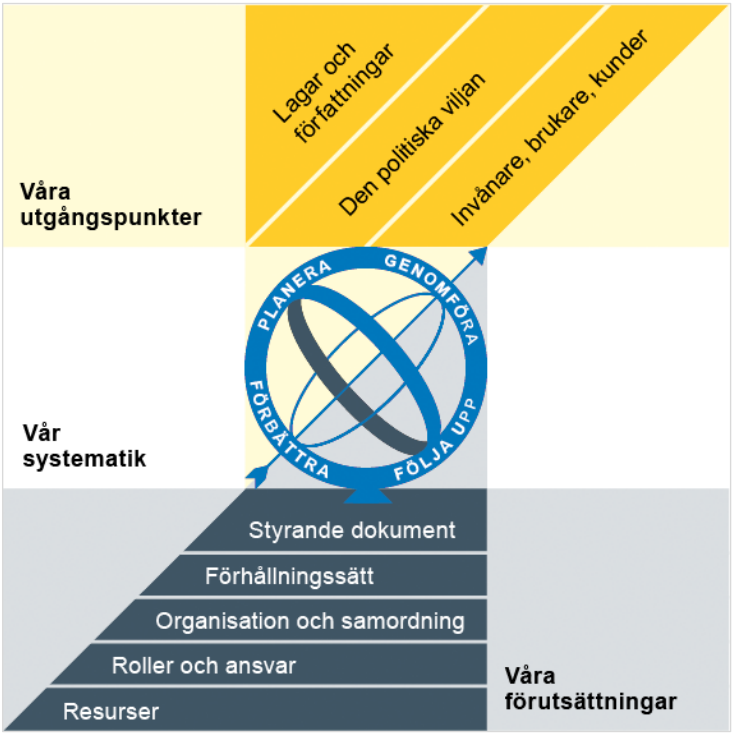
[Eventuell underrubrik]

Reglerande styrande dokument

- Policy
- Riktlinje
- Regel
- Anvisning
- ► **Rutin**
- Instruktion

Göteborgs Stads styrsystem

Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

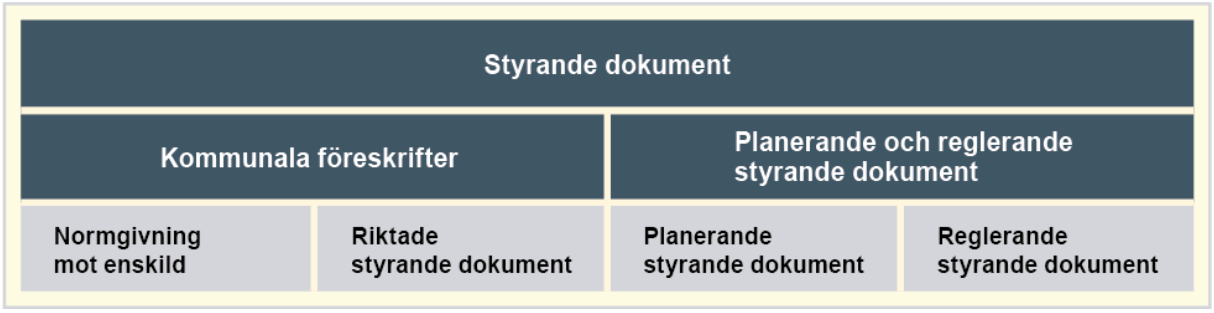


Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Dokumentnamn: Göteborgs Stads rutin för hantering av skyddade personuppgifter			
Beslutad av: [Nämnd/styrelse/befattning]	Gäller för: [Text]	Diarienummer: [Nummer]	Datum och paragraf för beslutet: [Text]
Dokumentsort: [Dokumentsort]	Giltighetstid: [Giltighetstid]	Senast reviderad: [Datum]	Dokumentansvarig: [Funktion]
Bilagor: [Bilagor]			

Innehåll

Inledning

Syftet med denna rutin

Hanteringen av skyddade personuppgifter inom Förvaltningen för Äldre, vård och omsorg

Vem omfattas av rutinen

Denna rutin gäller tillsvidare för Förvaltningen för Äldre, vård och omsorg

Bakgrund

Efter uppdrag från förvaltningsledningen för äldre, vård och omsorg har rutinen uppdaterats 2021-06-01

Koppling till andra styrande dokument

Rutinen är beslutad av förvaltningsledningen för äldre, vård och omsorg.

Angränsande dokument är: Förmedling särskilt boende, In-och utflyttning på särskilt boende-ÄBO, Informationsöverföring mellan Hälso-och sjukvård och socialtjänst (Regel), informationsöverföring mellan privata utförare och Göteborg stad (Rutin), Rutiner för hemtjänsten (Rutin), Journalföring inom hemsjukvården (Riktlinje)

Stödjande dokument

Bilaga 1: Checklista

Rutin

1. Generellt om skyddade personuppgifter

Någon som är utsatt för hot kan i vissa fall få skyddade personuppgifter. Det innebär att till exempel namnet och adressen skyddas i folkbokföringsregistret. I vanliga fall är uppgifterna i det svenska folkbokföringsregistret offentliga. Det finns tre typer av skyddade personuppgifter, eller skyddad identitet som det också kallas:

- skyddad folkbokföring, som har ersatt kvarskrivning
- sekretessmarkering
- fingerade personuppgifter, som innebär att du får nytt namn och personnummer.

Man ansöker om skyddad folkbokföring och sekretessmarkering hos Skatteverket. Fingerade personuppgifter ansöker man om hos Polisen.

1.1 Vad är skyddad folkbokföring?

Skyddad folkbokföring ger ett starkare skydd än sekretessmarkering. När det finns har en markering för skyddad folkbokföring får man vara folkbokförd i den gamla kommunen trots att man har flyttat därifrån, eller i en annan kommun som man inte har haft någon anknytning till. De gamla adressuppgifterna tas bort och den nya adressen registreras inte i folkbokföringen, och sprids därmed aldrig till andra myndigheter. En adress till Skatteverket registreras för brev och annan post till den enskilde.

Uppgifterna om skyddad folkbokföring skickas till andra myndigheter och annan samhällsservice som den enskilde har kontakt med, till exempel sjukvården, Försäkringskassan och kommunen. Det betyder att dessa instanser kan se att hen har skyddad folkbokföring.

1.2 Vad är sekretessmarkering?

En sekretessmarkering är den lägre graden av skyddade personuppgifter. En sekretessmarkering är en administrativ åtgärd som gör det svårare för andra att ta del av någons personuppgifter i folkbokföringsregistret. Sekretessmarkeringen omfattar alla personuppgifter.

En sekretessmarkering fungerar som en varningssignal för Skatteverket och andra myndigheter om att en prövning ska göras innan uppgifterna om personen lämnas ut. Det är alltså ingen absolut sekretess. En sekretessmarkering är en administrativ åtgärd som motsvarar hemligstämpeln på ett dokument.

Om en förföljd person själv lämnar sina personuppgifter till en myndighet måste personen själv informera myndigheten om att hen har en sekretessmarkering i folkbokföringen. Detta kan exempelvis ske genom att den enskilde bifogar en kopia av Skatteverkets beslut om sekretessmarkering till myndigheten. När Skatteverket lämnar ut uppgifter ur folkbokföringsdatabasen till andra myndigheter följer uppgift om sekretessmarkering med. När detta skett får det anses föreligga en särskild anledning för den mottagande myndigheten att göra en skadebedömning om de sekretessmarkerade uppgifterna begärs ut.

En sekretessmarkering hos Skatteverket utgör inte en slutlig prövning av sekretessfrågan. Den legala innebörden av en markering är att varje myndighet ska göra en noggrann

sekretessprövning vid en begäran om utlämnande av personuppgifter. Varje myndighet ska själv göra sekretessbedömningen. Vid bedömningen kan en myndighet alltså komma fram till att uppgifterna ska lämnas ut. (Hos socialtjänsten råder dock sekretess genom 26 kap. 1 § OSL, vilket innebär att uppgifterna även skyddas på det sättet.)

Det tar viss tid för Skatteverket att behandla en ansökan om sekretessmarkering. Om myndighetspersonalen får kännedom om sådana omständigheter som visar att hot riktats mot en enskild, bör sådana omständigheter kunna beaktas vid tillämpning av 21 kap. 3 § OSL (för dessa frågor se vidare prop. 2005/06:161, *Sekretessfrågor – skyddade adresser m.m.*, s. 55 f.).

1.3 Vad är fingerade personuppgifter?

Fingerade personuppgifter innebär att en person vid särskilt allvarliga hot kan få tillstånd att använda en annan identitet (se 1 § lag (1991:483) om fingerade personuppgifter).

Personen kan få fingerade personuppgifter om hen är utsatt för särskilt allvarlig brottslighet och hotas till livet, hälsa eller frihet. Det innebär att hen får nya identitetsuppgifter, till exempel ett nytt namn och ett nytt personnummer. Man ansöker om fingerade personuppgifter hos Polisen.

Av 21 kap. 3 § tredje stycket OSL följer att sekretess gäller för uppgift om koppling mellan fingerade personuppgifter och den enskildes verkliga personuppgifter, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Uppgifter om kopplingen mellan fingerad och verklig identitet skyddas alltså även om den enskilde i någon situation själv skulle lämna uppgifterna till en myndighet.

2. Skydd för personuppgifter i Treserva, behörigheter

Skyddade personuppgifter får inte förekomma i några andra IT-system än Treserva. I övrigt behandlas uppgifterna manuellt.

Intraservice får in aviseringar från Skatteverket varje dag. Om någon person i Treservas register har fått någon form av skydd för personuppgifter uppdateras detta automatiskt i Treserva.

Personens hela personnummer syns då inte längre i trädet och ärendet går inte att öppna. Det innebär att det inte går att komma åt ärendet.

Det finns två typer av skydd i Treserva: RSV-skydd och lokalt skydd. RSV-skyddet kommer från Skatteverket och är inget som kan påverkas av socialtjänsten. Även utan beslut från Skatteverket om skyddade personuppgifter kan socialtjänsten själv lägga ett lokalt skydd för ärenden i Treserva. Lokalt skydd används till exempel då det är en akut situation och personen inte har hunnit få skyddade personuppgifter via Skatteverket. Handläggare ansvarar för att meddela ett av de lokala verksamhetsstöden om att ett lokalt skydd behövs och lokalt verksamhetsstöd ansvarar därefter för att skyddet läggs in.

2.1 För område myndighet

Det bör maximalt vara tre personer per ärende som har behörighet till den enskildes uppgifter i Treserva. Lämpligen är detta ansvarig handläggare samt arbetsledning. Vid långvarig frånvaro eller handläggarbyte måste lokalt verksamhetsstöd informeras så att behörigheten tas bort.

2.2 För utförare

Risken för att sekretessmarkerade personuppgifter lämnas ut ökar med antalet personer som kan ta del av uppgifterna.

Så få personer som möjligt ska ha tillgång till ett ärende med skyddade personuppgifter, men tillräckligt många för att säkerställa ärendets handläggning vid frånvaro (semester, sjukfrånvaro, tjänstledighet). Inom vård- och omsorgsboenden samt korttidsvård behöver man till exempel säkerställa att någon personal har tillgång till nödvändig dokumentation under dygnets alla timmar.

Inom utförarverksamheterna måste en bedömning i varje enskilt fall göras utifrån verksamhetens karaktär.

2.3 Behörigheter för lokalt verksamhetsstöd

I Förvaltningen för äldre samt vård-och omsorg har fyra lokala verksamhetsstöd för Treserva behörighet att ge och ta bort behörighet i systemet gällande åtkomst av ärenden med skyddade personuppgifter.

2.4 Behörighet avgiftshandläggare

Personer med skyddad identitet ska inte förekomma i debiteringen i Treserva och ska inte läggas upp i något debiteringsområde. Beslutsmeddelandet om avgiften är generell och inte kopplad till avgiftsberäkningen. Uppgifter om avgiftsutrymmet kan läggas in manuellt. En avgiftsberäkning kan göras i Treservas utbildningsmiljö Alpha på en fiktiv person

Faktura till kund ska läggas upp manuellt i agresso då inga uppgifter går över från Treserva. För att avgiftshandläggaren ska få kännedom om en person med sekretesskydd måste hen bli kontaktad av biståndshandläggare.

Även utföraren måste ha kontakt med avgiftshandläggaren för att delge den utförda tiden. (alternativ att en person med skyddad identitet betalar för beviljad tid, beslut om undantag kan tas av verksamhetschef) En avgiftshandläggare behöver inte ha tillgång till uppgifter om den sekretesskyddade personer. Det finns dock ett undantag och det är om avgiftshandläggaren lägger upp kontraktet på ett vård-och omsorgsboende.

3. Kommunikation

Kommunikation med eller om personer med skyddade personuppgifter ska alltid ske via säkra kommunikationskanaler.

3.1 Brev

Brev till den enskilde skickas via Skatteverket, som i sin tur sänder brevet vidare. Brevet läggs i ett innerkuvert med personnumret utanpå. Innerkuvertet läggs sedan i ett ytterkuvert som skickas till (adressuppgift senast uppdaterad i juni 2021):

Skatteverket

Förmedlingsuppdrag

Box 2820

403 20 Göteborg

Inget annat än skattekontorets adress ska stå på det yttre kuvertet! Brevet inuti försändelsen förmedlas av Skatteverket till personen med adresskydd.

Skatteverket kan ha meddelat en annan särskild förmedlingsadress till personer som har skyddad folkbokföring. Använd i sådant fall den särskilda adressen.

För utskick till en person med sekretessmarkerade personuppgifter kan en myndighet även använda den adressuppgift som myndigheten själv förfogar över, om den enskilde givit sitt godkännande till detta.

3.2 Krypterad e-post

Kommunikation via e-post får i regel inte tillämpas i fråga om uppgifter som omfattas av sekretess, varken inom eller mellan myndigheter. E-post för extern kommunikation, till exempel med den enskilde, får endast användas om den enskilde själv vill att vi kommunicerar på detta sätt. Handläggare har ett ansvar att uppmärksamma den enskilde på riskerna med e-post.

Om e-post används som kommunikationsmetod, för att den enskilde vill det, är det av största vikt att mottagarfältet kontrolleras särskilt noga och att detaljerade adress- och kontaktuppgifter undviks. Använd krypterad e-post.

3.3 Fax

Ta först en telefonkontakt med den person som ska ta emot faxet. Kontakta mottagaren via telefon på nytt när faxet har skickats, för att bekräfta att det är mottaget. Spara mottagningsbeviset och förvara det i den fysiska personakten.

3.4 Internpost

Internpost kan användas under förutsättning att handlingen läggs i ett innerkuvert som läggs i internpostkuvertet. Bägge kuverten ska vara ordentligt förslutna och tydligt adresserade. Undvik adress-/kontaktuppgifter i handlingar som skickas med internpost.

3.5 Personligt besök

Säkerställ vid personligt besök att det är rätt person genom legitimation.

3.6 Telefon

Om personen inte är känd kan det vara nödvändigt att ha någon form av kod vid telefonkontakt. Denna måste då överenskommas vid ett personligt möte och skrivas ned i checklistan som ska ligga överst i den fysiska personakten.

Motring alltid andra myndigheter eller verksamheter, vid telefonkontakt.

3.7 Samsa

Enskild som har skyddad identitet registreras inte i IT-tjänsten SAMSA. Kontakt för vidare planering tas via telefon.

Dokumentation sker enligt regler för journalföring vid skyddad identitet i vardera vård- och omsorgsgivares journalsystem.

Om enskild med skyddad identitet sedan tidigare finns registrerad i IT-tjänsten SAMSA, ska folkbokföringsadress och personliga kontakter skyndsamt tas bort samt samtycken spärras.

3.8 Ingen rätt till anonymitet

Att den enskilde har skyddade personuppgifter innebär inte att personen är anonym i sin egen kontakt med socialtjänsten avseende sitt eget ärende.

4. Enhetschef och 1:e biståndshandläggare/samordnares ansvar

1. Ansvar för att alla medarbetare på enheten har kunskap om rutin samt om hur förvaring av skyddade personuppgiftsakter sker.

2. Ansvar för utlämnande av uppgifter gällande personer med skyddade personuppgifter (obs! vid begäran ställd till utförarverksamhet om utlämnande av skyddade personuppgifter, se 5.7.2).

3. Ansvar för att adress- och andra personuppgifter är borttagna innan de lämnas ut; detta gäller till såväl den enskilde som till annan mottagare (till exempel utskott/domstol, etc.). **Obs**! Även adress-/kontaktuppgifter är skyddade genom sekretessmarkering

4. Ansvar att tillse att ytterligare en person som har behörighet i ärendet kontrollerar att adress- och andra skyddade personuppgifter är borttagna på dokument innan utskick.

5. Ansvar för planering vid frånvaro (semester, tjänstledighet, etc.) gällande behörigheter samt sekretessprövning för handlingar innehållandes skyddade personuppgifter. I detta ingår att meddela lokalt verksamhetsstöd så att behörigheter i Treserva tas bort när så krävs.

5. Hantering av ärenden med skyddade personuppgifter

Handläggare och utförare har övergripande ansvar för att skyddet av den enskildes personuppgifter upprätthålls genom hela processen.

5.1 Ta emot ansökan/anmälan/kännedom på annat sätt samt aktualisering

Innan en ansökan eller anmälan hanteras som ett skyddat ärende måste en bedömning av den enskildes behov av skydd för personuppgifter göras.

Om skydd för personuppgifter inte längre behövs men det fortfarande finns kvar en sekretessmarkering, uppmanas den enskilde att kontakta Skatteverket för att ta bort den.

Sekretessmarkerade personer blir osynliga för alla användare i Treserva som inte har fått en särskild personlig behörighet till ärendet. Om handläggare försöker lägga till en person som har skyddade personuppgifter i aktualiseringen kommer meddelandet ”Behörighet saknas” och personen kan inte läggas till.

Om personen inte har haft ärende tidigare behöver lokalt verksamhetsstöd hjälpa till med aktualiseringen. Prata med ett lokalt verksamhetsstöd med behörighet att hantera åtkomst till skyddade personuppgifter.

1. personnummer och namn på den skyddade personen,
2. aktualiseringsuppgifter (enhet, mottagare, ärendetyp, avser anmälan eller ansökan m.m. orsak, ankomstsätt och ankom från, aktualiseringsdatum, eventuell text som ska stå i textrutan),
3. uppgifter om vem/vilka som ska vara behöriga (maximalt tre personer per ärende och enhet).

Lokalt verksamhetsstöd utför följande kontroller innan behörigheten ges:

- Är ärendet aktuellt i annan förvaltning i staden? Handläggare, som saknar den särskilda behörighet som lokalt verksamhetsstöd har, kan inte se om en skyddad person är aktuell i annan förvaltning.
- Har den enskilde kopplingar med andra personer i systemen? En skyddad person ”låser” även personer med kopplingar, så att dessa inte går att söka fram på vanligt sätt, även om de inte själva har skydd. Ofta har hela familjen samma skydd.

Lokalt verksamhetsstöd skapar därefter en aktualisering i Treserva, som endast kan ses av de personer som fått särskild behörighet. Handläggare måste logga ut och in igen för att behörigheten ska slå igenom.

Om en person som har pågående ärende i Treserva får sekretessmarkering hos Skatteverket uppdateras detta automatiskt i Treserva. Personens hela personnummer syns då inte längre i ”trädet” och ärendet går inte att öppna.

5.2 Riskbedöma och öppna utredning

Handläggare ska informera den enskilde om hur ärenden avseende personer med skyddade personuppgifter hanteras. Gör en skyddsbedömning.

Vid det första samtalet med den enskilde, tänk speciellt på och kom tillsammans med den enskilde överens om:

1. Hur hotbilden ser ut och hur skyddet behöver utformas (för hjälp med detta, se avsnitt 5.2.1 nedan).

Ge information om hur skyddade personuppgifter hanteras och vilka konsekvenser det kan få att ha skyddade personuppgifter.

Informera den enskilde om att vissa företag/myndigheter troligtvis inte är medvetna om att klienten har skyddade personuppgifter. Det är viktigt att den enskilde själv kontaktar myndigheter, organisationer och företag där personen finns registrerad för att berätta det. Den enskilde ska göras medveten om sitt eget ansvar för sin säkerhet och skydd av personuppgifter samt informeras om vikten av att inte i onödan lämna ut uppgifter om sig själv.

5.2.1 Riskbedömning och upprättande av rutin för enskild person

För varje enskilt ärende som rör en person med skyddade personuppgifter är det nödvändigt att kartlägga och bedöma hotbilden för att kunna utforma skyddet av

personuppgifter på ett korrekt sätt för just den personen. Generella rutiner i förvaltningen måste alltid kombineras med individuella rutiner som respektive enhet ansvarar för.

Till hjälp för detta finns en checklista som hittas under Styrande dokument (tillsammans med denna rutin) och som ska fyllas i och sedan läggas överst i den enskildes personakt. Checklistan ska uppdateras vid behov och stämmas av vid uppföljning av beslut.

De individuella rutinerna måste alltid bestämmas tillsammans med den enskilde. Handläggare ansvarar för att dokumentera informationen och de överenskommelser som görs.

5.2.2 Öppna utredning, förvaring av fysisk personakt

Om utredning inleds, öppnar handläggare ett skyddat ärende i Treserva och skapar en pappersakt (fysisk personakt). Den fysiska personakten ska förvaras skild från övriga akter i ett särskilt låsbart dokumentskåp i arkivet.

Akten ska vara inlåst i arkivskåp dygnet runt med undantag för när det pågår ett aktivt arbete i den.

5.2.3 Förhandsbedömning som inte leder till utredning

Förhandsbedömningar som inte leder till att utredning inleds ska tillföras en personakt eller sättas in i en pärm för handlingar som inte föranlett något ärende hos nämnden. Förhandsbedömningar som omfattar personer med skyddade personuppgifter ska, i de fall det inte finns en personakt, förvaras i pärm i särskilt låsbart dokumentskåp i arkivet.

5.2.4 Inhämta fakta och bedriva utredningsarbete

Genom hela processen ska de överenskommelser följas som gjorts med den enskilde (se punkt 5.2.1), bland annat kring hur kommunikation ska ske. Fundera särskilt över vilka kontakter som behöver tas under handläggningen för att tillräcklig information ska kunna inhämtas samtidigt som skyddet upprätthålls. Använd säkra kommunikationskanaler.

5.2.5 Byta handläggare i pågående ärenden

Prata med lokalt verksamhetsstöd. Följande uppgifter behövs:

1. Ärendenummer i Treserva.
2. Vem som ska läggas till respektive tas bort som behörig i ärendet.

5.2.6 Hantera tjänsteutlåtande/beslutsunderlag

Handläggare ansvarar för att det av tjänsteutlåtande/beslutsunderlag tydligt framgår att den enskilde har skyddade personuppgifter. På samtliga dokument (till exempel försättssida, utredning, vårdplan, genomförandeplan) ska anges att den enskilde har skyddade personuppgifter.

Endast den enskildes namn och personnummer ska finnas med i handlingarna. Undvik uppgifter som anger var den enskilde befinner sig, exempelvis boendeadress.

5.3 Uppmärksamhet vid kommunicering

Tänk särskilt på att en person kan ha skyddade personuppgifter i förhållande till anhöriga eller tidigare partner.

5.3.1 Fatta beslut

Sekretess hindrar aldrig en part i ett ärende från att få tillgång till ett beslut i ärendet.

Särskilda överväganden om utformningen av beslutet måste därför göras om det finns uppgifter om en part som inte bör komma till annan parts kännedom.

Om ärendet ska behandlas av nämnd/utskott måste alltid en särskild kontakt tas med respektive nämndsekreterare för att klargöra att ärendet omfattas av skydd.

5.3.2 Överklagat beslut/formulera och skicka uppdrag

Om beslutet överklagas är det viktigt att uppmärksamma domstolen på att den enskilde har skyddade personuppgifter. Handläggare ansvarar för att informera domstolen om skyddet.

Kontrollera att det inte finns med uppgift om boendeadress eller andra kontaktuppgifter i sakupplysningar och yttranden till domstol.

5.3.3 Formulera och skicka uppdrag

Handläggare ansvarar för att uppdraget överlämnas säkert via verksamhetssystem. Handläggare ansvarar också för att informera utförarverksamheten om att den enskilde har skyddade personuppgifter, om hur hotbilden ser ut samt om de överenskommelser som gjorts med den enskilde kring:

1. Hur skyddet behöver utformas, till exempel vid besök i hemmet, utflykter, fotografering, agerande vid akuta situationer.
2. Hur kommunikationen med den enskilde får ske.
3. Informera utföraren om vem/vilka som utföraren ska ha kontakt med på den myndighetsutövande enheten.
4. Komma överens om hur kommunikationen mellan ansvarig handläggare och ansvarig utförare ska gå till.

5.7 Förbereda och påbörja genomförande

Uppdragsmottagare går igenom uppdraget och ansvarar för att kontakta handläggaren för att diskutera eventuella oklarheter samt för att uppdraget fördelas till ansvarig utförare.

Rekommendation är att så få personer som möjligt ska ha tillgång till ärendet, men tillräckligt många för att säkerställa ärendets handläggning vid frånvaro (semester, sjukfrånvaro, tjänstledighet).

Pappersakter med sekretesskyddade personuppgifter ska förvaras åtskilda från övriga akter. En sådan akt ska vara inlåst i arkivskåp dygnet runt med undantag för när det pågår ett aktivt arbete i den. Dokumentation av de personer som har haft tillgång till akten ska ske.

5.7.1 Planera och genomföra planeringsmöte

För att biståndet ska kunna verkställas bör ett planeringsmöte hållas. Ansvarig handläggare kallar till planeringsmöte med den enskilde och ansvarig utförare.

Vid planeringsmötet ansvarar handläggaren för att tillsammans med den enskilde och utföraren gå igenom kartläggningen av den enskildes behov av skydd

Ansvarig utförare ansvarar för att vid planeringsmötet informera om hur skyddade personuppgifter hanteras och vilka konsekvenser det kan få att ha skyddade personuppgifter i utförarverksamheten.

Om en begäran om utlämnande av personuppgifter, som rör en person med skyddade personuppgifter, framställs till utförarverksamheten ska denna omedelbart vidarebefordra begäran till ansvarig handläggare för hantering.

5.8 Genomföra uppdrag, uppföljning

Ansvarig utförare ansvarar för att utföra uppdraget i enlighet med upprättad vårdplan/uppdrag samt överenskommen genomförandeplan. Under hela genomförandet är det viktigt att följa de överenskommelser som gjorts med den enskilde kring till exempel kommunikation och att följa de överenskommelser som gjorts med handläggaren kring hur kommunikationen mellan ansvarig utförare och handläggaren ska ske.

5.8.1 Uppföljning

Ansvaret för regelbunden uppföljning och utvärdering av genomförandet ligger hos ansvarig utförare.

Ansvaret för regelbunden uppföljning och utvärdering av behov och målet med beslutade insatser som helhet ligger hos ansvarig handläggare.

Uppgifter som anger var den enskilde befinner sig, såsom boendeadresser, ska i möjligaste mån undvikas i de handlingar som upprättas i samband med uppföljning. Följ den överenskommelse som gjorts för hur kommunikationen mellan ansvarig utförare och handläggare ska gå till vid säker överlämning av handlingar mellan enheterna.

Vid varje gemensam uppföljning ansvarar handläggare för att särskilt följa upp skyddsbehovet, vilket kan förändras över tid.

5.9 Avsluta insats och ärende samt överlämna ärende till annan myndighet

Handläggare avslutar insatsen (och om så är aktuellt även ärendet) i Treserva. Meddela lokalt verksamhetsstöd att ärendet har avslutats. Lokalt verksamhetsstöd tar då bort de särskilda behörigheterna i ärendet.

Avslutade akter avseende personer med skyddade personuppgifter ska förvaras på säker plats, inlåsta och åtskilda från andra akter .

5.9.1 Överlämna ärende till annan kommun

Vid överlämning av ett ärende till annan kommun ansvarar handläggaren för att säkerställa att mottagaren får kännedom om skyddsbehovet och de överenskommelser som gjorts kring skyddet. Använd säkra kommunikationskanaler vid överlämnandet.

6. Internkontroll och avvikelser

6.1 Egenkontroll ska genomföras avseende:

- Regelbundet följa upp att regler och rutiner kring skyddade personuppgifter så att regler följs och respekteras
- Loggranskning

6.2 Avvikelser

Rapportera risker och avvikelser som ”ej person” i Treservas digitala avvikelsemodul.