Hantering av skyddade personuppgifter

Policy

Strategi

▶ Riktlinje

Plan

Laholms kommun
Postadress: 312 80 Laholm. Besöksadress: Humlegången 6
Växel: 0430-150 00. www.laholm.se

Beslutad av:	Diarienummer:	Typ av styrdokument:	Dokumentansvarig:
Kommunstyrelsen	2025-000290	Riktlinje	HR och Lön
Beslutsdatum och paragraf:	**Giltig till:**	**Senast reviderad:**	
2025-10-14 § 220	Tillsvidare	2025-10-14	

Innehållsförteckning

Innehållsförteckning 2
1. Syfte....3
2. Koppling till lagstiftning och andra styrdokument 3
3. Skyddade personuppgifter 4
Vad är skyddade personuppgifter 4
Den anställdes anmälningsskyldighet 4
4. Hantering av arbetssökande med skyddad identitet vid rekrytering....5
Central hantering av anställd med skyddad identitet efter rekrytering 5
Chefens praktiska hantering: 6
Information till medarbetare med skyddad identitet.... 6
5. Begäran av allmän handling 8
6. Ansvar och uppföljning 8
Bilaga 1 Checklista för medarbetare med skyddade personuppgifter 9
Bilaga 2 Instruktioner till IT-service 10
Bilaga 3 Rutin för hantering av arbetssökande med skyddade personuppgifter....11

1. Syfte

Uppgifter om en person i folkbokföringen, bostadsadress, telefonnummer, e-post med mera är i regel offentliga. En person som, om sådana uppgifter offentliggörs, kan antas utsättas för hot, våld eller annan allvarlig händelse men kan dock få sina personuppgifter skyddade. Syftet med denna anvisning är tydliggöra hur Laholms kommun ska hantera personuppgifter för anställda med skyddade personuppgifter och vart man ska vända sig.

2. Koppling till lagstiftning och andra styrdokument

Skyddade personuppgifter är en samlingsrubrik som Skatteverket använder för de olika skyddsåtgärderna sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter inom folkbokföringen.

Enligt 22 kap. 1 § offentlighets- och sekretesslagen (OSL) är uppgifter inom folkbokföringsverksamheten i regel offentliga. I vissa fall kan det dock skada en person att uppgifter om denne lämnas ut. Det kan t.ex. gälla någon som är hotad eller förföljd.

Av 21 kap. 3 § OSL framgår att sekretess gäller för uppgift om en enskilds bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde bor stadigvarande eller tillfälligt, den enskildes telefonnummer, e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med denne samt för motsvarande uppgifter om den enskildes anhöriga. Om det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs.

3. Skyddade personuppgifter

Vad är skyddade personuppgifter

Det finns tre typer av skyddade personuppgifter, eller skyddad identitet som det också kallas:

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

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 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 lämnas ut. Det är alltså ingen absolut sekretess. En sekretessmarkering är en administrativ åtgärd som motsvarar hemligstämpeln på ett dokument.

Skatteverket kan registrera en sekretessmarkering om det finns risk för att personen utsätts för brott, förföljelse eller allvarliga trakasserier. En sekretessmarkering är vanligtvis giltig i två år.

Skyddad folkbokföring

Skyddad folkbokföring ger ett starkare skydd än sekretessmarkering.
När en person har en markering för skyddad folkbokföring är den folkbokförd på en annan folkbokföringsort än där personen är bosatt. De flesta väljer att vara folkbokförda i den gamla kommunen trots att de har flyttat därifrån.

Skyddad folkbokföring beslutas av Skatteverket och medges som regel för obestämd tid. Åtgärden kan dock begränsas till viss tid om det finns särskilda skäl för det.

Fingerade personuppgifter

En person kan få fingerade personuppgifter om hen är utsatt för särskilt allvarlig brottslighet och hotas till sitt liv, hälsa eller frihet. Det innebär att hen får nya identitetsuppgifter, till exempel ett nytt namn och ett nytt personnummer. Normalt sett får kommunen inte kännedom om att en person har fingerade personuppgifter.

Den anställdes anmälningsskyldighet

En person som har skyddade uppgifter måste själv upplysa om att hen har skyddad folkbokföring eller sekretessmarkering. När någon med skyddade personuppgifter nyanställs eller när en medarbetare får skyddade uppgifter ska hen visa upp Skatteverkets beslut.

4. Hantering av arbetssökande med skyddad identitet vid rekrytering

I den centrala hanteringen utav rekryteringen till Laholms kommun så finns i varje annons som publiceras information gällande inlämning utav ansökningshandlingar från personer med skyddad identitet. Dessa ansökningshandlingar ska alltid gå direkt till chef och inte registreras i Laholms kommuns rekryteringssystem Varbi. Ansökningshandlingarna ska hanteras säkert utav chef och inte registreras.

Central hantering av anställd med skyddad identitet efter rekrytering

När en person som ska nyanställas talar om att hen har skyddade personuppgifter ska anställande chef ha ett möte där information ges och blankett för skyddad identitet fylls i och undertecknas. Medarbetaren ska visa dokumentation från Skatteverket om att hen har en skyddad identitet. Kopia ska förvaras i personalakt. Är personens ansökan under handläggning kan Skatteverkets bekräftelsemeddelande uppvisas och beslut inlämnas när det är klart. Vid nyanställning ska en legitimationskontroll göras.

Verksamheten för HR och Löns systemförvaltare är utsedda till att hantera registrering i personalsystemen och där lägga till en anonymitetsspärr så att personuppgifterna med automatik inte flyttas till andra system. Central personalakt förvaras så att den endast kan tas fram av ett fåtal medarbetare på Verksamheten för HR och Lön. Personalakten förvaras inte digitalt utan endast i pappersform i låst arkivskåp.

Medarbetare och chef har vid nyanställning ett samtal där de går igenom hur medarbetaren kan hantera sin digitala identitet. De går igenom checklistan (bilaga 1) där de antecknar det alias namn medarbetaren önskar använda i de system där autentiska uppgifter inte krävs. Lönechef antecknar sedan det TF-personnummer (tillfällig födelsedata) som ska användas. Checklistan där koppling mellan autentiska och alias/TF uppgifter finns sparas i personalakten.

Digitalt ID och e-postadress skapas manuellt genom att systemförvaltare gör en beställning hos IT-service med en tydlig notering kring vilken form utav skydd personen har det vill säga vilket namn som ska stå i mejladressen. IT-service ska hantera uppgifter kring medarbetare med skyddad identitet på ett säkert och skyddat sätt. Alias och TF-personnummer ska användas. IT-service förmedlar användar-ID, e-post och lösenord för medarbetaren till chef via telefon eller säkra meddelanden. Medarbetaren ändrar sedan lösenordet till ett personligt.

Övriga system som medarbetaren behöver tillgång till hanteras i dialog mellan chef, systemförvaltare och aktuell förvaltning. Detta kan ske via ärendehanteringssystem som finns tillgängliga genom IT samt Verksamheten för HR och Lön.

När medarbetaren slutar meddelas att den skyddade identiteten ska upphöra till systemförvaltare som kontaktas utav medarbetarens chef i dessa frågor Ska personens handlingar sekretessbeläggas utifrån sina personuppgifter ska det finnas grund till detta, till exempel utifrån det skyddet som personer innehar.

De dokument med personuppgifter som arbetsplatsen är i behov av har chef ett ansvar för att de hanteras på ett säkert och skyddat sätt så att inga uppgifter kan spridas.

Chefens praktiska hantering:

- Håll direkt kontakt med systemförvaltare på Verksamheten för HR och Lön och meddela medarbetarens person- och anställningsuppgifter. Lämna kopia på Skatteverkets beslut. Systemförvaltare registrerar i personalsystemet och skapar anställningsavtal. Ansökningshandlingar och underskrivit anställningsavtal ska sedan förmedlas till anställd på lön som hanterar personalakten. Om det under anställningen krävs nytt anställningsavtal kontaktas systemförvaltare. Papper som ska förvaras i medarbetarens personalakt lämnas till aktuell person på Verksamheten för HR och Lön.
- Boka samtal med medarbetaren där du går igenom information ”3.1.4 Information till medarbetare med skyddad identitet” samt hur medarbetaren kan hantera sin digitala identitet. Chef informerar även kring GDPR och dess skydd för personuppgifter, samt fördjupat kring personer med skyddad identitet. Ni antecknar det alias som medarbetaren önskar använda samt om medarbetarens systembehov avviker från det normala. Checklistan (bilaga 1) ska signeras och sedan lämnas till systemförvaltare. Samt stäm av hur person ställer sig person till vara kontaktperson, synas på bild, digitala medier
- IT-service kontaktar anställande chef när Digital ID, e-post och lösenord är klart.
- Barn- och utbildnings- samt socialförvaltningen som har speciella kontaktpersoner som hanterar behörighetsupplägg i verksamhetssystem för medarbetare med skyddad identitet. Systemansvarig förmedlar uppgifter till dessa. Socialförvaltningen fyller i och undertecknar ordinarie behörighetsblankett som lämnas till Verksamheten för HR och Lön för arkivering. För övriga förvaltningar görs en avstämning mellan chef och systemansvarig kring vilka system som behövs och vilka uppgifter som behöver förmedlas.
- Anhöriguppgifter ska förvaras i slutet kuvert på säker plats hos dig som närmsta chef.
- Ska du skicka brev till medarbetaren sker det enligt Skatteverkets förmedlade rutiner (se adress nedan).
- När medarbetaren slutar eller om medarbetaren meddelar att den skyddade identiteten ska upphöra, kontaktar du lönechef som ansvarar för förmedling av informationen till berörda så att behörigheter och digitalt konto avslutas.

Information till medarbetare med skyddad identitet

Du har för din chef uppvisat beslut och lämnat kopia från Skatteverket om att du har skyddade personuppgifter. För att kunna arbeta i Laholms kommun krävs att dina personuppgifter hanteras både i pappersform och digitalt. De kommer att begränsas så mycket som möjligt och hanteras av få personer.

När du nyanställs eller meddelar att du har fått skyddade personuppgifter har du ett samtal med din chef. Under samtalet informeras du om hur Laholms kommun hanterar dina personuppgifter och ni går igenom vilka behov/begränsningar just din situation kräver. Ni uppdaterar ett dokument kring din digitala identitet där eventuellt alias framgår.

- Central personalakt förvaras så att den endast kan tas fram av ett fåtal medarbetare på Verksamheten för HR och Lön. Personalakten förvaras inte digitalt utan endast i pappersform.
- De dokument med personuppgifter som arbetsplatsen och närmsta chef är i behov av hanteras på ett säkrare så att inga uppgifter kan spridas.
- Uppgifter i personalsystemet läggs in och anonymitets skyddas. Då kan endast ett fåtal medarbetare på Verksamheten för HR och Lön ta del av dessa.
- Inga personuppgifter förs med automatik från personalsystemet till andra system.
- Digitalt ID och e-postadress skapas manuellt. I mailadressbok visas alias eller namn, titel, arbetsplats och förvaltning.
- Autentiska uppgifter används i de system där de behövs, då är de registrerade på ett skyddat sätt. I övriga system används alias namn och TF-personnummer (födelsedata).
- Sändning av brev till dig från Laholms kommun sker enligt Skatteverkets förmedlande rutiner.
- Anhörigregister förvaras i slutet kuvert hos närmsta chef och skulle situationen för den anställde förändras är det viktigt att den anställde inkommer med denna information till chef.
- I bilaga 1 kan önskemål till chef läggas gällande till exempel hantering utav bilder som sedan sparas i akt.

Hantering av post till personer med skyddade personuppgifter

De brev som ska förmedlas ska läggas i ett slutet kuvert. Kuvertet ska ha uppgift om avsändaradress så att Skatteverket kan returnera försändelsen om mottagaren inte kan nås. När möjlighet till säkra meddelanden inom digital post är tillgängligt, så används detta.

På kuvertet ska du skriva mottagarens personnummer och, om möjligt, mottagarens fullständiga namn.

Lägg kuvertet i ett ytterkuvert och skriv Skatteverkets förmedlingsadress på det yttre kuvertet. Flera försändelser kan givetvis läggas i samma ytterkuvert.

Posten kommer att förmedlas till mottagaren oavsett var mottagaren bor.

Skatteverkets förmedlingsuppdrag
Box 2820
403 20 GÖTEBORG

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

5. Begäran av allmän handling

Vid begäran av allmän handling som innefattar person med skyddad id

- Vid lönelistor döljer systemet personen
- Vid utlämnande av övriga uppgifter, ska känsliga uppgifter maskas utifrån persons nivå utav personuppgiftsskydd.

6. Ansvar och uppföljning

Varje nämnd, ansvarar för att denna anvisning efterlevs. Uppföljning sker vart tredje år av Verksamheten för HR och Lön.

Bilaga 1 Checklista för medarbetare med skyddade personuppgifter

- Jag har för min chef uppvisat och lämnat kopia på beslut från Skatteverket som styrker att jag har skyddade personuppgifter.
- Jag har tagit del av informationen om hur Laholms kommun hanterar personuppgifter för en medarbetare med skyddad identitet.
- Jag och min chef har gått igenom vilka behov/begränsningar min situation kräver och antecknat dem i denna checklista.
- Jag är informerad om att denna checklista sparas i min personalakt.

Personnummer		Namn	

Utifrån denna beskrivning över kommunövergripande system gör jag följande ställningstagande.

System (Obligatoriska)	**Så här visas uppgifter**
Personalsystem (Personec, WinLas, Adato, TimeCare)	Namn är anonymitetsskyddat
AD/ARS Mail	Namn, befattning, arbetsplats och förvaltning visas, ☐ Jag vill att alias namn visas och används i mailadress

Övriga upplysningar kring systembehov eller annat som avviker från normal användaren i liknande befattning:

Alias namn och TF kommer att användas där det är möjligt, där det behövs autentiska uppgifter ansvarar systemförvaltare för att personuppgifterna är skyddade.

☐ HSA - SITHS	Jag önskar att uppgifter visas ☐

Jag önskar följande **alias namn**: _____

Datum _____

_____ _____

Medarbetarens underskrift Chefs underskrift

_____ _____

Namnförtydligande Namnförtydligande

Bilaga 2 Instruktioner till IT-service

Medarbetare med skyddad identitet förs inte med automatik över från personalsystemet till AD/ARS för skapande av digital Identitet utan ska skapas manuellt efter uppgifter från chef för Verksamheten för HR och Lön. IT-enheten ska meddela kontaktperson/er till chef för Verksamheten för HR och Lön.

- Chef för Verksamheten för HR och Lön kontaktar IT-service och förmedlar de uppgifter som behövs. (TF-personnummer, alias namn, förvaltning, arbetsplats, chef)
- IT-enheten lägger upp konto manuellt, alias och TF-personnummer ska användas.
- Titel, arbetsplats och förvaltning registreras och används i adressbok.
- IT-enheten förmedlar användar-ID till chef för Verksamheten för HR och Lön.
- IT-enheten förmedlar användar-ID, mailadress och lösenord till chef.
- Chef för Verksamheten för HR och Lön förmedlar avslut eller förändrad chef/förvaltning till IT-enheten.
- Chef för Verksamheten för HR och Lön går två gånger per år igenom personer med skyddad identitet för att se att de fortfarande är anställda och att chefsuppgift är rätt och förmedlar ändringar till IT-enheten.

Instruktioner till utsedda kontaktpersoner för skyddade personuppgifter samt systemförvaltare:

Behörighetstilldelning för personer med skyddad identitet sker inte utefter vanliga rutiner utan hanteras manuellt då uppgifter inte bör föras mellan system.

Alias och TF-personnummer (födelsedata) ska användas om inte systemet kräver autentiska uppgifter.

Om autentiska uppgifter behöver vara registrerade i systemet ansvarar systemförvaltare att dessa uppgifter hanteras på ett säkert och skyddat sätt.

Bilaga 3 Rutin för hantering av arbetssökande med skyddade personuppgifter

En person som är utsatt för ett allvarligt och konkret hot kan ansöka om skyddade personuppgifter hos Skatteverket. Det finns tre typer av skyddade personuppgifter (även kallat skyddad identitet): sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter. Här kan du läsa mer om vad dessa innebär.

Om en arbetssökande har skyddade personuppgifter hos Skatteverket ska vi som arbetsgivare erbjuda en så säker ansökningsprocess som möjligt. Det är viktigt att endast ett fåtal personer hos arbetsgivaren hanterar den arbetssökandes uppgifter. Vi bör minimera antalet inblandade personer så att vi ökar skyddet för den arbetssökande.

1. **Mottagande av ansökan**

Arbetssökande med skyddade personuppgifter uppmanas via platsannons att ta kontakt med angiven rekryterande chef för att guidas vidare till en säker ansökningsprocess. Arbetssökande ska uppmanas att skicka in ansökan i pappersformat till rekryterande chef.

2. **Förvaring och diarieföring av ansökningshandlingar**

Ansökningshandlingarna förvaras inlåsta under rekryteringsprocessen hos rekryterande chef. Rekryterande chef lägger in eller kontaktar Verksamheten för HR och Lön som lägger in kandidaten i rekryteringssystemet genom att döpa kandidaten till ”Skyddade personuppgifter”. Detta för att kandidaten inte ska missas under rekryteringsprocessen samt vid diarieföringen. Observera att ansökningshandlingarna inte ska registreras i rekryteringssystemet.

Vid erhållen tjänst skickar rekryterande chefansökningshandlingarna till Lönechef på HR-avdelningen som förvarar ansökningshandlingarna i personalakt.

Vid ej erhållen tjänst skickar rekryterande chefansökningshandlingarna till chef på Verksamheten för HR och Lön som bevarar ansökningshandlingarna inlåsta i 2 år innan gallring. HR anger vilken tjänstansökan avser med referensnummer och annonsrubrik.

3. **Begäran om utlämnande av allmän handling**

Vid utlämnande av ansökningshandlingar så sekretessprövas begäran av HR med stöd av kommunjurist.

4. **Anställning av person med skyddade personuppgifter**

För fortsatt säker hantering vid anställning av person med skyddade personuppgifter ta kontakt med din förvaltnings HR-Konsult.