Anvisningar för generell hantering av skyddade personuppgifter inom arbetsmarknadsnämndens verksamheter

Bakgrund

Arbetsmarknadsnämnden beslutar om dessa anvisningar utifrån Stockholms stads ”Stadsövergripande policy om skyddade personuppgifter med riktlinjer till nämnder och bolag”.

Anvisningarna utgår från en riskbedömning av de skyddade personuppgifter som nämnden behandlar och konsekvensen av om dessa uppgifter lämnas ut till en obehörig person. Anvisningarna är till för att säkra att de skyddade personuppgifter som återfinns i verksamheterna registreras, hanteras och förvaras på ett säkert och enhetligt sätt.

Utöver dessa anvisningar finns även särskilda styrdokument som redogör för hur arbetsmarknadsnämnden och arbetsmarknadsförvaltningen hanterar informationssäkerhetsfrågor och behandling av personuppgifter. I samband med att behandling av personuppgifter påbörjas, ska även rutiner för hantering av skyddade personuppgifter tas i beaktande. Även andra lagstiftningar och styrdokument kan behöva tas i beaktande i samband med hantering av personuppgifter.

Vad innebär ”skyddade personuppgifter”?

Skyddade personuppgifter innebär att någon form av skyddsåtgärd har vidtagits för att göra någons personuppgifter mindre tillgängliga, oftast därför att ett hot mot personen föreligger. En personuppgift är varje typ av uppgift som kan härledas till en nu levande individ. Det finns tre typer av skyddsåtgärder:

- Sekretessmarkering.
- Skyddad folkbokföring (tidigare ”kvarskrivning”)
- Fingerade personuppgifter

Sekretessmarkering innebär som hörs på ordet att det finns en markering som signalerar att den enskildas personuppgifter ska

Arbetsmarknadsförvaltningen
Administrativa staben

Livdjursgatan 4, Johanneshov
Box 10014
12126 Stockholm-Globen
Telefon 08-508 35 511
Växel 08-508 35 500
Fax 08-508 35 542
info.amf@stockholm.se
stockholm.se

behandlas med försiktighet. Ofta framgår det inte exakt vilken personuppgift (till exempel namn eller adress) som är skyddsvärd. Denna markering meddelas andra myndigheter via Skatteverket. *Skyddad folkbokföring* betyder att personen är folkbokförd på en adress som den inte (längre) bor på. Post till denna person går då via en särskild adress på Skatteverket. *Fingerade personuppgifter* innebär att personen får helt nya personuppgifter och att inga kopplingar finns till de gamla.

Sekretessmarkering och skyddad bokföring beslutar Skatteverket om och fingerade personuppgifter beviljas av polisen.

Ansvarsfördelning

Arbetsmarknadsförvaltningen ansvarar för att ta fram förslag till nämnden på anvisningar för generell hantering av skyddade personuppgifter som gäller för samtliga verksamheter inom förvaltningen.

Till anvisningarna hör även tre rutiner; en rutin gällande generell hantering av skyddade personuppgifter samt en rutin för respektive verksamhetsavdelning som gäller verksamheterna inom den avdelningen. Förvaltningschef beslutar om den generella rutinen, och för respektive avdelnings rutiner beslutar ansvarig avdelningschef.

Varje verksamhetsavdelning inom förvaltningen ansvarar för att rutiner för hantering av skyddade personuppgifter finns för varje verksamhet, antingen gemensamma rutiner på avdelningsnivå eller enhetsspecifika rutiner. Framtagande av dessa avdelningslokala rutiner sker utifrån ”Stadsövergripande policy om skyddade personuppgifter med riktlinjer till nämnder och bolag”, ”Anvisningar för hantering av skyddade personuppgifter inom arbetsmarknadsnämnden” samt ”Arbetsmarknadsförvaltningens generella rutin för hantering av skyddade personuppgifter”.

Avdelningarna ska i framtagandet av lokala rutiner ta särskild hänsyn till och utgå från särskilda bestämmelser gällande tillexempel verksamhetsspecifik lagstiftning och styrdokument eller verksamhetsspecifik sekretess.

Hantering av personuppgifter

Arbetsmarknadsnämnden/arbetsmarknadsförvaltningen ska inte i onödan ta med information om personuppgifter i handlingar och information. Varje verksamhet har därför som ansvar att kontinuerligt se över vilken information som ovillkorligen måste

anges i ansökningar, beslut, protokoll och andra typer av handlingar/information. Hanteringen ska följa de styrdokument och rutiner som gäller vid hantering av personuppgifter inom arbetsmarknadsnämnden/arbetsmarknadsförvaltningen.

I arbetsordningar, anvisningar och dylikt eftersträvas vanligen en rationell och enhetlig handläggning av ärenden och det finns då risk för att skyddade personuppgifter i onödan krävs in eller tas in i en handling. Rådande lagstiftning gällande hantering av personuppgifter, Dataskyddförordningen (GDPR), anger att personuppgifter som inte behövs inte heller ska begäras in. För att undvika detta ska styrdokument och rutiner gällande hantering av personuppgifter efterlevas av nämndens verksamheter.

Hantering av personuppgifter och skyddade personuppgifter i IT-stöd

Arbetsmarknadsnämnden/arbetsmarknadsförvaltningen och dess verksamheter ska särskilt beakta hanteringen av skyddade personuppgifter vid utveckling av IT-stöd. Det kan till exempel gälla att:

- Säkerställa att endast ett fåtal personer, som har behov av behörighet, ska kunna att ta del av skyddade personuppgifter.
- En tydlig utmärkning av sekretessen bör finnas i varje bildskärmsfönster där uppgifter om en person med skyddade personuppgifter redovisas. Det bör framgå om det rör sig om sekretessmarkering eller skyddad folkbokföring.
- Vid behov kunna se vilken handläggare som tagit del av uppgifter om personer med skyddade personuppgifter.

Vid utveckling av IT-stöd eftersträvas alltmer system med enhetliga rutiner och med små möjligheter till avvikelser. För att inte tappa kontrollen över skyddade personuppgifter ska behandlingen av sådana uppgifter särskilt beaktas vid systemutvecklingen. Konsekvensbedömningar utifrån GDPR samt informationssäkerhetsklassningar bidrar till att säkerställa att hantering av skyddade personuppgifter tas i beaktande.

För att säkerställa att verksamheten har korrekt information om personuppgifter ska i första hand de verktyg/system som finns tillgängliga användas, till exempel BER och FLAI.

I de system som hanterar personuppgifter ska det tydligt gå att utläsa om uppgifter är skyddade och om det rör sig om sekretessmarkering eller skyddade personuppgifter.

IT-stödet ska vara utformat så att endast ett fåtal personer, som har behov av behörighet, ska kunna att ta del av skyddade personuppgifter. Risken för att skyddade personuppgifter lämnas ut, av misstag eller medvetet, ökar med antalet handläggare/användare som kan ta del av uppgifterna, och denna risk ska alltid minimeras. Detta gäller vid såväl direktåtkomst på bildskärm som uttag av uppgift på papper.

Tillgång till skyddade personuppgifter

Kretsen av personer som har behörighet att ta del av skyddade personuppgifter ska begränsas så mycket som möjligt. Enbart de handläggare/användare som har behov av uppgifterna ska kunna ta del av skyddade personuppgifter. Detta gäller oavsett om uppgifterna finns i ett IT-stöd eller på papper.

Förvaring och markering av skyddade personuppgifter

Skyddade personuppgifter ska, oavsett om de är digitala eller i pappersformat, förvaras och markeras på ett enhetligt och tydligt sätt inom verksamheten för att minimera risken för eventuella misstag. Om lokala rutiner behövs för att säkerställa detta ansvarar verksamheten för att ta fram sådana rutiner. För en användare som har behörighet att ta del av skyddade uppgifter ska det på ett säkert och enhetligt sätt framgå att uppgifterna är skyddade.

Det är viktigt att markeringar om skyddade personuppgifter syns vid alla sökningar i register och att de markeras tydligt både på bildskärm och i pappersform.

Kommunikation innehållande information om skyddade personuppgifter

Kommunikation med och om personer med sekretessmarkerade personuppgifter ska ske på ett säkert sätt utifrån de beslutade anvisningarna. Om osäkerhet gällande kommunikation finns kontaktas förvaltningens administrativa stab för rådgivning.

Skyddade personuppgifter ska inte spridas till områden där sekretess för uppgifterna inte föreligger. Personer med skyddade personuppgifter ska informeras om vikten av att inte i onödan lämna ut uppgifter om sig själva.

Verksamheten ska vända sig till den enskilde eller till exempel andra myndigheter endast via en säker kommunikationskanal. Säkra kommunikationskanaler är brev med mottagarbevis/rekommenderat brev, elektronisk kommunikation med hjälp av elektronisk

legitimation och personligt besök av den enskilde där hen legitimerar sig.

Kommunikation via e-post ska inte tillämpas i fråga om skyddade personuppgifter, vare sig inom eller mellan myndigheter.

Kommunikation med andra myndigheter per telefon kan vara möjlig efter motringning.

För utskick till en person med sekretessmarkerade personuppgifter kan en myndighet använda den adressuppgift som myndigheten själv förfogar över.

Om det inte finns någon adressuppgift i verksamheten, till exempel där verksamhetsspecifik sekretess inte finns, och brev behöver skickas till en person med skyddade personuppgifter kan försändelsen överlämnas till Skatteverket, som i sin tur sänder försändelsen vidare till berörd person i Skatteverkets tjänstekuvert. Adressuppgifter till Skatteverkets förmedlingskontor finns på Skatteverkets hemsida under ”Information om skyddade personuppgifter”. Där framgår även hur den praktiska hanteringen ska gå till.

Möjligt att i efterhand kontrollera vilka handläggare som har tagit del av skyddade personuppgifter

Kontroll är viktig för att i efterhand kunna spåra vilken eller vilka handläggare/användare som har tagit del av uppgifter om en person med skyddade personuppgifter. Detta kan till exempel ske genom kontroll av loggar. Handläggare/ användare ska informeras om att kontroller genomförs.

Regelbunden uppföljning av efterlevnad av anvisningar och rutiner kring skyddade personuppgifter

Arbetsmarknadsnämnden/arbetsmarknadsförvaltningen genomför i samband med internkontroll efterlevnad av de styrdokument och rutiner som gäller för hantering av skyddade personuppgifter. Verksamheten ska själva genomföra årlig egenkontroll gällande hantering av personuppgifter utifrån rådande styrdokument och rutiner.