Stadsövergripande policy om skyddade personuppgifter med riktlinjer till nämnder och bolag

Inledning

Inom stadens verksamheter hanteras en stor mängd personuppgifter. Personuppgifter kan efter beslut av skatteverket vara skyddade. Det är angeläget att stadens verksamheter hanterar skyddade personuppgifter på ett enhetligt och säkert sätt. Varje nämnd i staden måste därför göra en noggrann genomgång av sin verksamhet och upprätta anvisningar för hanteringen av skyddade personuppgifter inom den egna verksamheten om så krävs utöver denna stadsövergripande policy. Med nämnd avses i det följande även kommunala bolag.

Beroende på arten av hot finns det tre grader av skyddade personuppgifter. Skyddade personuppgifter är samlingsnamnet som skatteverket använder för åtgärderna sekretessmarkering, kvarskrivning och fingerade personuppgifter**.**

Sekretessmarkering

Enligt 22 kap. 1 § offentlighets- och sekretesslagen (2009:400, OSL), är uppgifter inom folkbokföringsverksamheten i regel offentliga. Sekretess gäller om det av särskild anledning kan antas att en person, eller någon närstående, kan lida skada eller men om uppgiften om personen lämnas ut.

I de fall skatteverket på förhand kan bedöma att utlämnande av uppgifter om en person kan orsaka personförföljelse eller annan skada kan en s.k. markering för särskild sekretessprövning (sekretessmarkering) sättas för personen i folkbokföringsdatabasen.

Det framgår inte av själva markeringen vilken uppgift om personen i folkbokföringen som kan vara känslig. Det behöver inte bara vara adressen som är den skyddsvärda uppgiften, det kan även vara nytt namn eller uppgifter om närstående.

Markeringen ska fungera som en varningssignal så att en noggrann prövning görs innan några uppgifter om personen lämnas ut. En sekretessmarkering innebär inte någon absolut sekretess. Vid en begäran om utlämnande av personuppgifter ska

varje myndighet göra en självständig sekretessbedömning. Vid bedömningen kan myndigheten komma fram till att uppgifterna ska lämnas ut.

Skatteverket aviserar sekretessmarkeringen till andra myndigheter tillsammans med övriga uppgifter om personen, när uppgifterna lämnas över till myndigheterna.

Kvarskrivning

Ett annat sätt att skydda personuppgifter i folkbokföringen är att genom beslut om kvarskrivning medge en person vid flyttning att vara folkbokförd på den gamla folkbokföringsorten i högst tre år.

Kravet för en person att få bli kvarskriven är att han av särskilda skäl kan antas bli utsatt för brott, förföljelser eller allvarliga trakasserier på annat sätt. Omständigheterna ska i princip motsvara de som gäller för meddelande av besöksförbud enligt lagen (1988:688) om besöksförbud.

Vid kvarskrivning framgår inte den verkliga bostadsorten av folkbokförings-registret och därmed sprids den inte heller till aviseringsmottagarna. Den gamla adressen tas bort och personen registreras ”på församlingen skriven”. Skatteverkets adress anges som en särskild postadress.

Det som aviseras till andra myndigheter är en flyttning där personen blivit på församlingen skriven och med den särskilda postadressen. Någon annan särskild markering aviseras inte. All post går då till skatteverket som har den faktiska adressen manuellt förvarad och kan vidarebefordra posten.

Kvarskrivningen fungerar som ett adresskydd. Men i regel får en kvarskriven person också en sekretessmarkering. Då aviseras även sekretessmarkeringen.

Fingerade personuppgifter

Vid särskilt allvarliga hot kan en person medges att använda annan identitet. Beslut om detta meddelas av Stockholms tingsrätt efter ansökan hos Rikspolisstyrelsen. Den nya identiteten registreras på ett sådant sätt att det inte framgår att det rör sig om fingerande personuppgifter. Kopplingen mellan identiteterna finns endast hos Rikspolisstyrelsen.

Nedan följer riktlinjer till nämnder och bolag om hantering av skyddade personuppgifter.

Riktlinjer till nämnder och bolag om hantering av skyddade personuppgifter

Med nämnd avses i det följande även kommunala bolag.

1. Varje nämnd ska utforma anvisningar om hanteringen av skyddade personuppgifter inom den egna verksamheten, om så krävs utöver dessa riktlinjer.

Nämnderna ska utforma sina anvisningar utifrån en egen riskbedömning av de skyddade personuppgifter som myndigheten behandlar och konsekvensen av om dessa uppgifter lämnas ut till en obehörig person.

Nämnder med likartade verksamhetsområden, som t.ex. stadsdelsnämnderna, kan ha gemensamma anvisningar för hanteringen av skyddade personuppgifter inom dessa verksamhetsområden.

Nämnder som inte omfattas av någon form av verksamhetsspecifik sekretess ska om möjligt inte registrera skyddade personuppgifter, eftersom uppgifterna kan bli offentliga och en nämnd kan bli skyldig att lämna ut t.ex. en adress. Anställda med skyddade personuppgifter måste dock registreras bl.a. för att administrera löneutbetalningar. Det finns emellertid allmänna bestämmelser gällande sekretess för personuppgifter i 21 kap. OSL som är tillämpliga inom alla myndigheters verksamheter, men varje myndighet ska själv göra en sekretessbedömning och myndigheten kan då komma fram till att uppgiften är offentlig.

Alla nämnder som hanterar skyddade personuppgifter i verksamheten ska registrera och förvara sådana uppgifter på ett säkert och enhetligt sätt.

E-tjänst, e-post

Den enskilde med skyddade personuppgifter ska alltid upplysas om risken med att lämna ut sina uppgifter, t.ex. ska den enskilde informeras om riskerna med att hantera elektroniska tjänster och e-post. Nämnderna ska vid behov kunna erbjuda alternativ till e-hantering av personuppgifter.

2. Nämnderna ska inte i onödan ta med information i sina handlingar.

Varje nämnd bör göra en översyn av vilken information som ovillkorligen måste anges i ansökningar, beslut, protokoll och andra handlingar.

I arbetsordningar, anvisningar o.d. 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. Enligt personuppgiftslagen ska personuppgifter som inte behövs inte heller begäras in.

3. Varje nämnd ska särskilt beakta hanteringen av skyddade personuppgifter vid utveckling av IT-stöd.

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 system-utvecklingen.

Elektroniskt Personregister Stockholm Stad (EPS), vilket är under utveckling, ska tillhandahålla stadens verksamheter och e-tjänster så korrekta personuppgifter som möjligt. EPS ska användas som masterdatabas vid nyanskaffning av informations-system. Äldre redan driftsatta system, ska också använda EPS som källa för personuppgifter så långt som möjligt.

Det ska tydligt gå att utläsa om uppgifter är skyddade i de system som hanterar personuppgifter.

4. Varje nämnd ska utforma IT-stödet så att endast ett fåtal personer har behörighet 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. Detta gäller vid såväl direktåtkomst på bildskärm som uttag av uppgift på papper.

Kretsen av personer som har behörighet att ta del av skyddade personuppgifter ska därför begränsas så mycket som möjligt. Enbart de handläggare/användare som har behov av uppgifterna ska kunna ta del av skyddade personuppgifter.

5. 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.

Sekretesskyddade personuppgifter ska förvaras och markeras på ett enhetligt och tydligt sätt inom verksamheten, både digitalt och manuellt, för att minimera risken för eventuella misstag.

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.

6. Varje nämnd ska utforma enhetliga och säkra rutiner för att kommunicera med och om personer med sekretessmarkerade personuppgifter.

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.

Nämnden ska vända sig till den enskilde eller t.ex. andra myndigheter endast via en säker kommunikationskanal. Säkra kommunikationskanaler är brev, elektronisk kommunikation med hjälp av elektronisk legitimation och personligt besök av den enskilde om han eller hon har legitimerat 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 man inte har någon adressuppgift i verksamheten, t.ex. där verksamhetsspecifik sekretess inte finns, och man behöver skriva till en person med skyddade personuppgifter kan försändelsen överlämnas till skatteverket, som i sin tur sänder försändelsen vidare till berörd person i skatteverkets tjänstekuvert. Adresser till skatteverkets förmedlingskontor finns på www.skatteverket.se under skyddade personuppgifter. Där framgår även hur den praktiska hanteringen ska gå till. På varje nämnd ska det finnas rutiner för kommunikation via skatteverket.

8. Det ska vara möjligt att i efterhand kontrollera vilka handläggare som har tagit del av skyddade personuppgifter.

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

9. Varje nämnd ska regelbundet följa upp att dess regler och rutiner kring skyddade personuppgifter efterlevs inom den egna nämnden.

Varje nämnd ansvarar för att anvisningarna för hantering av skyddade personuppgifter följs.
