Rekommendation för hantering av uppgifter som omfattas av sekretess i Säker digital kommunikation

Innehåll

1. Inledning

Informationssäkerhetsarbetsgruppen SDK har tagit fram en rekommendation för hur uppgifter som omfattas av sekretess ska hanteras vid användning av Säker digital kommunikation (SDK). Rekommendationen omfattar även hur personuppgifter för personer med skyddade personuppgifter ska hanteras.

Syftet är att få till en enhetlig hantering hos användarorganisationer. Enhetliga rutiner underlättar hanteringen inom den offentliga förvaltningen och minskar risken för att uppgifter som omfattas av sekretess och skyddade personuppgifter oavsiktligt lämnas ut eller hamnar i orätta händer.

2. Rekommendation om hantering av uppgifter som omfattas av sekretess

2.1 Arbetsgruppens rekommendation

Myndigheter i Sverige ska samarbeta med och utlämna information till varandra.
Dock får utbytet av information inte ske helt fritt. För att en sekretessbelagd uppgift ska kunna lämnas till en annan myndighet krävs det att en sekretessbrytande bestämmelse är tillämplig.

Såväl avsändande som mottagande organisation gör sin bedömning av eventuella sekretessgrunder. Mottagande organisation kommer vid ett utlämningsärende att göra en egen bedömning. I det kommer avsändande organisations bedömning beaktas, men inga garantier kan lämnas om att respektive mottagande organisations bedömning överensstämmer med avsändande organisation.

För att möjliggöra enkla och tydliga rekommendationer för användare av SDK men samtidigt ge ett adekvat skydd vid hantering av uppgifter som omfattas av sekretess föreslår arbetsgruppen följande arbetssätt.

1. Om avsändande organisation bedömer att ett meddelandes innehåll inklusive eventuella bilagor omfattas av sekretess ska den nyttja funktionen ”omfattas av sekretess”[1] som en markering till den mottagande organisationen.

   Den avsändande organisationen ska i meddelandets fritextfält ange vilken information som den anser omfattas av sekretess samt med motivering till bedömningen.

2. Om meddelandet rör personer med skyddad identitet ska funktionen ”omfattas av sekretess” nyttjas och hänvisning ska göras till
   - 21 kap. 3 § OSL och 22 kap. 2 § OSL för sekretessmarkering
   - 16 § FOL, 21 kap. 3 och 3 a§§ OSL och 22 kap. 2 och 3 §§ OSL för skyddad folkbokföring.

   Om avsändande organisation inte har information om personens skyddsnivå kan hänvisning göras till som minst 21 kap. 3 § OSL och 22 kap. 2 § OSL

   Se även nedan i avsnitt 3 Rekommendation om hantering av skyddade personuppgifter.
3. Observera att mottagande organisation alltid är ansvarig för att göra en bedömning av om meddelandet omfattas av sekretess även om ”omfattas av sekretess” inte har använts av avsändande organisation.

[1] Funktionen ”omfattas av sekretess” innebär att användaren anger om meddelandets innehåll omfattas av sekretess eller ej.

3. Rekommendation om hantering av skyddade personuppgifter

3.1 Vad är skyddade personuppgifter

Uppgifterna som registreras i folkbokföringen är som huvudregel offentliga. I vissa fall kan det dock skada en person att uppgifter om denne lämnas ut. Det kan till exempel gälla den som riskerar att utsättas för brott, förföljelser eller allvarliga trakasserier. Skatteverket kan då välja mellan att registrera två olika typer av markeringar i folkbokföringsdatabasen:

- Sekretessmarkering
- Skyddad folkbokföring (har ersatt det som tidigare kallades kvarskrivning)

Sekretessmarkering är en varningssignal om behovet av att göra en noggrann skadeprövning enligt 22 kap. 1 § offentlighets- och sekretesslagen, OSL, när någon begär att få ut en sekretessmarkerad uppgift. Adress är i regel den uppgift som är mest skyddsvärd, men även andra uppgifter inom folkbokföringen kan behöva skyddas, till exempel uppgifter om anhöriga och uppgifter som kan röja var personen eller dennes anhöriga kan befinna sig. Uppgift om namn är ofta skyddsvärd. Det kan vara förödande för en person som har bytt namn i syfte att stärka sitt skydd om det nya namnet sprids i samhället.

En markering för skyddad folkbokföring registreras i folkbokföringsdatabasen. Personen är folkbokförd på en annan folkbokföringsort än där personen är bosatt. Någon bostadsadress registreras inte utan endast en särskild postadress. Den särskilda postadressen är en boxadress som går till ett skattekontor.

3.1.1 Individens ansvar

Den som har skyddad folkbokföring eller sekretessmarkerade personuppgifter i folkbokföringen måste vara mycket noga med hur hen hanterar sina uppgifter. Till exempel behöver den som har skyddade personuppgifter själv kontrollera om en uppgift som lämnas till en myndighet blir sekretesskyddad hos myndigheten. Personen måste också själv upplysa om att hen har skyddad folkbokföring eller sekretessmarkering.

3.1.2 Skatteverkets vägledning

Varje användarorganisation bör genom en riskanalys klarlägga hur skyddade personuppgifter ska behandlas inom den egna verksamheten och tillse att Skatteverkets vägledning efterlevs. Ur Skatteverkets vägledning framgår bland annat att ”myndigheter inom samma verksamhetsområde bör kunna ha gemensamma anvisningar för hanteringen av skyddade personuppgifter”. Det framhålls att det är viktigt att det görs skillnad på vilka uppgifter som har markering för skyddad folkbokföring och vilka uppgifter som har sekretessmarkering.

3.2 Arbetsgruppens rekommendation

Rekommendationen bygger på den mer generella rekommendationen som arbetats fram av ett flertal regioner i samråd med bland annat Nationellt center för kvinnofrid och Skatteverket för hantering av personer med skyddade personuppgifter inom regionerna. I korthet går dessa rekommendationer ut på att personnummer/samordningsnummer ska användas i så stor utsträckning som möjligt, även för personer med skyddade personuppgifter.

Ur Skatteverkets vägledning framgår att det är viktigt att det görs skillnad på uppgifter som har markering av skyddad folkbokföring och vilka uppgifter som har sekretessmarkering. Detta bör dock uppnås inom användarorganisationen och är inte ett krav i informationsutbytet mellan användarorganisationer. Det är möjligt att hantera skydden lika, vilket innebär att båda skyddsnivåerna får ett högre skydd.

För att möjliggöra enkla och tydliga rekommendationer för användare av SDK men samtidigt ge ett adekvat skydd för personer med skyddade personuppgifter föreslår arbetsgruppen följande arbetssätt.

1. Om personuppgifter avseende personer med skyddade personuppgifter, oavsett skyddsåtgärd, ska skickas via SDK ska endast personnummer/samordningsnummer överföras med begränsad möjlighet till undantag. Rekommendationen är att inte använda namn, men det kan vara möjligt efter att riskanalys genomförts inom respektive användarorganisation.

2. Den begränsade möjligheten till undantag ska vara väl beskriven, vilket innebär att rutiner för när och hur avsteg kan vara möjligt ska tas fram av respektive användarorganisation. Det kan finnas behov av att stämma av avsteg med mottagande användarorganisation.

3. Varje användarorganisation bör ta fram tydlig information till personer med skyddade personuppgifter.

4. I SDKs referensfält ska i första hand ärendenummer och i andra hand personnummer/samordningsnummer användas. Namn och kontaktuppgifter ska inte användas.