

Socialnämnden i Botkyrka Kommun

147 785 Tumba

Tillsyn enligt personuppgiftslagen (1998:204) – Utökat elektroniskt informationsutbyte

Datainspektionens beslut

Datainspektionen förelägger Socialnämnden i Botkyrka kommun (Socialnämnden), som en förutsättning för att kunna använda Multifråga (direktåtkomst) att:

1. införa tekniska begränsningar i Multifråga, som innebär att handläggarna hos Socialnämnden endast kan ta del av personuppgifter hos Försäkringskassan (FK) och Centrala studiestödsnämnden (CSN) som behövs för de pågående ärenden som finns hos Socialnämnden, samt
2. ta fram rutiner som möjliggör åtkomstkontroll av direktåtkomsten i Multifråga, och även utföra åtkomstkontroller i Multifråga.

Datainspektionen förutsätter att Socialnämnden utvärderar och kontinuerligt utvecklar logguppföljningarna av direktåtkomsten i Multifråga för att uppnå en verkningsfull åtkomstkontroll.

Ärendet avslutas, men kan komma att följas upp.

Bakgrund

Den 1 januari 2009 trädde ett antal nya bestämmelser i kraft som innebär ett utökat elektroniskt informationsutbyte mellan myndigheter (se prop. 2007/08:160). Informationsutbytet ska huvudsakligen ske genom s.k. direktåtkomst. Datainspektionen inledde under 2010 ett projekt för att hos två socialnämnder och två statliga myndigheter granska hur informationsutbytet ser ut och om tillämpliga bestämmelser följs. Inspektionerna har inte föranletts av något klagomål mot socialnämnderna eller myndigheterna, utan är ett led i Datainspektionens projekt. Av särskilt intresse har varit systemens utform-

ning och datakommunikation, information till registrerade och hanteringen av skyddade personuppgifter.

Redogörelse för tillsynsärendet

Datainspektionen har den 26 oktober 2010 genomfört en inspektion hos Socialnämnden. Närmare uppgifter om vad som framkommit i ärendet och därmed legat till grund för Datainspektionens bedömning framgår av skälen till beslutet. Datainspektionen har efter inspektionen inhämtat kompletterande handlingar.

Tillämpliga rättsregler m.m.

Bestämmelserna om behandling av personuppgifter i socialnämndernas verksamhet i 6 § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten och 12 § första stycket p. 1 förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten, reglerar den behandling av uppgifter som informationsutbytena med bl.a. CSN och FK innebär. Utöver dessa bestämmelser blir även 31 § personuppgiftslagen aktuell vad gäller de tekniska och organisatoriska åtgärderna för att skydda de personuppgifter som behandlas.

Av 6 § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten framgår att personuppgifter får behandlas bara om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten ska kunna utföras. En registrerad person har inte rätt att motsätta sig sådan behandling av uppgifter som är tillåten enligt denna lag.

Det framgår vidare av 12 § första stycket p. 1 förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten att en kommunal myndighet får behandla personuppgifter för handläggning av ärenden om bistånd och annat stöd samt genomförande av beslut om bistånd, stödinsatser, vård och behandling samt annan social service som följer av bestämmelserna i socialtjänstlagen (2001:453) och 2 kap. 7 § lagen (2009:47) om vissa kommunala befogenheter.

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av:

- de tekniska möjligheter som finns,
- vad det skulle kosta att genomföra åtgärderna,
- de särskilda risker som finns med behandlingen av personuppgifterna, samt
- hur pass känsliga de behandlade personuppgifterna är.

Skäl för beslutet

Allmänt om informationsutbytet

Socialnämnden har för närvarande ett informationsutbyte med FK och CSN. För informationsutbytet använder Socialnämnden sig av en webbtjänst som Sambruk har tagit fram, Multifråga.

Kravet på försäkran från Socialnämnderna – FK och CSN

Datainspektionen vill upplysningsvis informera om gällande registerförfattningar, vad gäller FK och CSN. Enligt bestämmelsen som sedan den 1 januari 2011 finns i 114 kap. 22 § socialförsäkringsbalken (2010:110) får en socialnämnd ha direktåtkomst först sedan FK har försäkrat sig om att handläggare hos Socialnämnden bara *kan* ta del av uppgifter om personer som är aktuella i ärenden hos nämnden. Av 13 § studiestödsdataförordningen framgår motsvarande krav gentemot CSN.

Bestämmelserna ovan är riktade till myndigheterna, men anger även en förutsättning för vad som gäller för socialnämndernas direktåtkomst till myndigheternas personuppgifter. I tillägg är socialnämnderna skyldiga att, i enlighet med 31 § personuppgiftslagen, vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas.

Det har i ärendet framkommit att FK inte inhämtat någon skriftlig försäkran om att Socialnämnden har vidtagit de tekniska åtgärder som krävs för att säkra att anställda vid Socialnämnden, vid direktåtkomst till personuppgifter som behandlas hos FK, endast kan ta del av uppgifter som är aktuella i ärenden hos Socialnämnden.

Det har vidare framkommit att Socialnämnden skriftligen försäkrat CSN om att Socialnämnden har vidtagit de tekniska och administrativa åtgärder som krävs för att säkra att anställda vid Socialnämnden, vid direktåtkomst till personuppgifter som behandlas i CSN:s studiestödsverksamhet, bara kan ta del av uppgifter som är aktuella i ärenden hos Socialnämnden. Socialnämnden har även försäkrat att behandlingshistorik förs som visar vilken anställd hos Socialnämnden som har berett sig tillgång till personuppgifter som behandlas i CSN:s studiestödsverksamhet.

Det har även framkommit att det endast är medlemmar i gruppen "Ekonomiskt bistånd" som har åtkomst till Multifråga, men att det inte finns några tekniska begränsningar i "Multifråga" som gör att det endast går att söka på personer i pågående ärenden.

Datainspektionen kan konstatera att även om FK inte har försäkrat sig om att Socialnämnden har vidtagit de tekniska åtgärder som krävs, saknas det tekniska begränsningar i Multifråga som innebär att handläggarna endast kan ta del av uppgifter om personer som är aktuella hos Socialnämnden.

Datainspektionen konstaterar vidare att Socialnämnden har försäkrat CSN om att Socialnämnden har vidtagit de tekniska och administrativa åtgärder som krävs för att anställda vid Socialnämnden endast kan ta del av uppgifter som är aktuella i ärenden hos Socialtjänsten. Vid inspektionstillfället framkom dock att det saknas tekniska begränsningar i "Multifråga" som gör att det endast går att söka på vissa personnummer.

Mot bakgrund av dessa brister förelägger Datainspektionen Socialnämnden att, som en förutsättning för att kunna använda Multifråga (direktåtkomst), införa tekniska begränsningar i Multifråga, som innebär att handläggarna hos Socialnämnden endast kan ta del av personuppgifter hos FK och CSN som behövs för de pågående ärenden som finns hos Socialnämnden.

I detta sammanhang vill Datainspektionen även erinra Socialnämnden om att lagstiftaren har förutsatt att socialnämnderna i sin arbetsordning eller motsvarande dokument ska ange vilka personer som för vilka syften har behörighet att för myndighetens räkning ta del av de uppgifter som anges i de sekretessbrytande bestämmelserna (se Regeringens prop. 2007/08:160, Utökad elektroniskt informationsutbyte, s. 141).

Upplysningsvis informeras Socialnämnden om att FK, i Datainspektionens beslut dnr 1523-2010, har förelagts att upphöra med att ge socialnämnderna åtkomst till uppgifter ur socialförsäkringsdatabasen via LEFI Online, till dess att FK försäkrat sig om att handläggare hos socialnämnderna bara kan ta del av uppgifter om personer som är aktuella i ärenden hos nämnden. Vidare har CSN, i Datainspektionens beslut dnr 1735-2010, förelagts att upphöra med att lämna ut uppgifter om enskilda via direktåtkomst till Socialnämnden, till dess att CSN – även på annat sätt - försäkrat sig om att handläggare hos Socialnämnden rent tekniskt inte ska ha möjlighet att söka på andra personer än sådana som är aktuella i ett ärende hos Socialnämnden.

Behörighetsstyrning

Det har framkommit att alla handläggare, i Socialnämndens ärendehanteringssystem, har teknisk åtkomst till alla ärenden men att handläggarna inte får öppna de personakter som de inte handlägger. Det har vidare framkommit att det är oklart hur ofta behörighetskontona går igenom, men att detta uppskattningsvis sker oftare än en gång per år. Antalet aktiva konton överens-

stämmer inte helt med det aktuella antalet, då ca tio behörigheter ännu inte har hunnit avslutas.

Datainspektionen kommer, inom ramen för det pågående tillsynsärendet, inte att ta ställning till Socialnämndens behörighetsstyrning enligt ovan. Däremot kan Datainspektionen komma att handlägga denna fråga särskilt.

Behandlingshistorik och åtkomstkontroll

I enlighet med 31 § personuppgiftslagen är Socialnämnden, i egenskap av personuppgiftsansvarig, skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas.

Det har framkommit att loggen från Multifråga bl.a. innehåller uppgifter om tidpunkt, vilken handläggare som ställde frågan, ärende-id, hushålls-id och omfrågade person/samordningsnummer. Det går således att utreda vem som gjorde vad och när. Det går också att kontrollera mot verksamhetssystemet att det fanns ett ärende vid den tidpunkt då frågan ställdes. Det har vidare framkommit att det för närvarande inte görs någon åtkomstkontroll av direktåtkomsten i Multifråga, men att det för närvarande diskuteras hur man ska göra.

Datainspektionen kan konstatera att Socialnämnden för närvarande inte utför någon åtkomstkontroll av direktåtkomsten i Multifråga.

Mot bakgrund av denna brist förelägger Datainspektionen Socialnämnden att ta fram rutiner som möjliggör åtkomstkontroll av direktåtkomsten i Multifråga, och även utföra åtkomstkontroller i Multifråga. Vidare förutsätter Datainspektionen att Socialnämnden utvärderar och kontinuerligt utvecklar logguppföljningarna av direktåtkomsten i Multifråga för att uppnå en verkningsfull åtkomstkontroll.

Särskilt om skyddade personuppgifter

Datainspektionen har i tidigare tillsynsbeslut uttalat att för att obehöriga inte ska komma åt skyddade personuppgifter är det bland annat viktigt att det vid myndigheter finns sekretessmarkeringar som syns tydligt vid sökningar i register, att all personal som hanterar personuppgifter ges grundlig information om skyddade personuppgifter och sekretessfrågor, att kretsen av personer som har tillgång till skyddade personuppgifter begränsas så mycket som möjligt, att skyddade personuppgifter inte sprids till områden där sekretess för uppgifterna inte föreligger och att myndigheten regelbundet följer upp att regler och rutiner kring skyddade personuppgifter efterlevs och respekteras.

Det har framkommit att muntlig information ges kontinuerligt till handläggarna om hur skyddade personuppgifter ska hanteras i systemet. Detta går även igenom vid utbildning av nya handläggare.

Alla ärenden med skyddade personuppgifter hanteras i ett särskilt distrikt till vilket endast vissa handläggare har behörighet. Alla med behörighet dit kan se alla ärenden som finns i distriktet. Det är den handläggare som handlägger ärendet, dennes chef och den som betalar fakturan som har rätt att titta på uppgifterna.

När det gäller Socialnämnder som ingår i Sambruk, lämnar FK inte ut någon information om personer som har skyddade personuppgifter. Handläggaren får i detta fall kontakta FK för att erhålla uppgifterna. Beträffande skyddade personuppgifter hos CSN lämnar CSN ut dessa uppgifter till Socialnämnden, men det framgår då av informationen från CSN att personuppgifterna omfattas av sekretess.

Datainspektionen har inget att erinra mot hanteringen av skyddade personuppgifter.

Information till de registrerade om informationsutbytet m.m

Det framgår av prop. s. 140 att lagstiftaren bl.a. förutsätter att de enskilda dels blir tydligt informerade om informationsutbytena mellan myndigheterna, dels får del av uppgifter som Socialnämnden inhämtar och tillför ärendet innan det enskilda ärendet avgörs, om avgörandet går parten emot (jmf 17 § förvaltningslagen).

Det har i ärendet framkommit att de enskilda blir informerade om det pågående informationsutbytet i ansökningsblanketten/samtyckeshandlingen, som fylls i en gång per månad. De enskilda blir även informerade av handläggarna om att det görs kontroller genom Multifråga hos FK och CSN. Det framgår av handlägningsrutinerna att information om dessa kontroller måste ske.

Varje månad skickas beräkningsunderlaget hem till den enskilde, dvs. underlaget till beslutet. Detta görs oavsett om beslutet går den enskilde emot. Den enskilde får även muntligen information om beräkningen innan beslutet fattas.

Datainspektionen har i denna del inget att erinra.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder över klagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, teamledaren Britt-Marie Wester, IT-säkerhetsspecialisten Magnus Bergström samt juristerna Lena Carlsson och Maria Bergdahl, föredragande.

Göran Gräslund

Maria Bergdahl

Kopia till:

1. CSN
2. FK
3. Sambruk